



使用者手冊



BitDefender 網路安全 2009

BitDefender 網路安全 2009
使用者手冊

出版 2008.12.08

法律聲明

BitDefender 網路安全 2009






內容目錄











使用者軟體授權合約

如果您不同意這些條款和條件，請勿安裝此軟體。若在安裝前選擇了「我同意」、「確定」、「繼續」、「是」等選項，代表您完全了解及接受這份合約上的條款。

產品註冊。當接受此合約，您會同意使用"我的帳號"註冊您的產品，作為您產品使用與維護的條件。這個管控確保軟體只會在有效授權的電腦上使用，有效授權的使用者才能享有維護的服務。註冊需要一組有效的授權序號以及有效的電子郵件帳戶以使用續購優惠及其他法律條款。

對您來說，這個條款含概了 BitDefender 家用使用者的解決方案及服務，包含了相關的文件及任何應用程式的更新及升級，在您所購買的授權或任何相關的服務協定都定義在這份文件及任何這些條款的複本。

對於您與 BITDEFENDER 公司來說，這份授權合約是份法律協議，在您使用 BitDefender 的軟體產品，它將涵概了電腦軟體、服務，可能也包含了相關的媒體、列印的手冊及線上或電子式的檔案，而這些都將被國際著作權法及國際商標法所保護。在安裝、複製及使用 BitDefender 時，您將同意這個協定上的條款。

如果您不同意這個合約的條款，請不要安裝或使用 BitDefender。

BitDefender 授權。. 像智慧財產權法律及條款一樣，BitDefender 被著作權法律及國際著作權條款所保護。BitDefender 是使用授權而非賣斷。

授權取得。BITDEFENDER 提供您非獨一的、有限的、不可轉移的使用 BitDefender 授權。

軟體的使用。您可以按合約所訂的授權數量上安裝 BitDefender 軟體於許多電腦上。您也可以製作一份額外的複製光碟以備份為用途。

桌上型電腦使用者授權。這個 BitDefender 軟體授權可以安裝在個人電腦上，它並沒有提供網路服務。每個使用者可以安裝這個軟體在一台個人電腦，而且可以製作一份額外的複製當備份用途。主要使用者的數量依授權書上的使用者授權數量。

授權期限。BitDefender 軟體的使用授權於購買日起至軟體到期日止。

使用期滿。當使用期滿時，產品會立即停止執行它的功能。

升級。如果BitDefender標示為升級版，您必須按照合約上規定正確地使用。如果是標示為升級替換或產品補助亦是您升級版的合格依據。您可以按使用合約上規定使用此升級版。 如果BitDefender升級只是整個產品的部分，您仍舊被授權使用單一產品，BitDefender或許可以被部分使用或傳遞但仍不可超過合約規定的使用數量。升級版的條款可能會取代或修改原先您與BitDenfender的原始條款。

版權。BitDefender之所有權利、標題、以及著作權 (包含任何影像、相片、企業標識、動畫、影片、聲音、音樂、文字及BitDefender內之applets),與列印的材料、及 BitDefender 的任何複製版都屬 BITDEFENDER 公司所擁有。BitDefender 受到著作權法律及國際條款所保護。您必須對待 BitDefender 像其他有版權的媒體一樣。您不可以複製任何 BitDefender 附屬的檔案。您必須在所有包含 BitDefender 的複製媒體,附上所有的版權聲明。您不可再授權、租、售或分享 BitDefender 的授權。您不可利用反向工程、反編譯、拆解及建立衍生品、修改或解譯 BitDefender 原始程式碼。

有限保證。BITDEFENDER 保證從您收到 BitDefender 產品的 30 日內,可享有免費軟體媒體瑕疵更換的權利。BITDEFENDER 提供保證在收到瑕疵品後,可以選擇更換媒體或退還您購買 BitDefender 的金額。BITDEFENDER 不保證 BitDefender都沒有錯誤或錯誤都會被修正。BITDEFENDER 亦不保證 BitDefender 將符合您所有的需求。

除了合約書上明確的規定外,BitDefender不負責產品其他的明確或暗示性的保證包含改進、維護、支援或有形與無形的材料與服務。 BitDefender 明確地不對任何無限責任,適用於任何特定用途的保證、標題、資料與訊息內容準確性,以及過濾、中斷、清除其他公司軟體間諜程式、廣告、郵件、 cookies 與檔案擔負責任。無論是法令規章、交易條款、慣例與商業用途所導致的。

損害聲明。 任何人使用、測試、評估BitDefenderd可能存在影響BitDefender品質、性能上之風險,BitDefender 將不負任何責任。 BitDefender不對任何損害負責,包含無限的直接或間接使用上的損害,性能或傳送Bitdefender甚至是BitDefender已告知可能存在的損害。BitDefender所負責任將不超過您購買BitDefender的代價。以上聲明與有限責任,您自行決定是否接受使用,評估或測試BitDefender。

某些州不允許限制或排除對偶然損失或必然損失的責任,因此上述限制或排除可能不適用於您

BITDEFENDER的責任將不會超過您支付購買BITDEFENDER產品的價值金額。上述的免責條款和限制將會應用在不論是使用、評估或是測試BitDefender。

用戶重要通知. 本軟體不是容錯的也不是設計用在損壞時會自動啟動的作業環境。本軟體不適用於飛航作業,核能管控或通信系統、武器系統,直接或間接的生命支援監控系統或任何會導致死亡或身體,財產嚴重傷害之系統 。

電子通信同意書。. BitDefender會需要發送給您法律通知與其它關於軟體與維護授權服務的通信資訊,或是您提供給我們的資料的使用途徑。BitDefender將會透過產品內的聲明、或最初使用者註冊時使用的電子郵件帳號、或是公布在網站上發送通訊資料。接受此同意書,您將會同意只使用這些方式接受通信資訊,認可並表示您可以於網站存取信資訊。

一般條款。本合約受羅馬尼亞及國際版權之管轄。如有任何違反條款其裁決管轄為羅馬尼亞法院。

BitDefender的價格、費用與酬金如有變動是不會預先通知您的。

本合約的任一條款如有失效，此 一失效的條款將不影響本合約的其他條款的有效性。

BitDefender與其logos是屬BitDefender之商標，在本產品用到所有其他商標與相關的材料屬其他個別公司所有。

如您違反任何條款，本合約將立即終止且不予事先通知。而您也得不到BitDefender或其經銷商任何賠償，且合約條款有關使用上之保密與限制依然有效。

BitDefender可在任何時間修改條款，而修正後的條款將自動地在推出的相關版本的軟體使用且不影響其他條款的有效性。

在各種翻譯語文如有爭議或不一致性時，以BitDefender的英文版條款為基準。

聯絡 BITDEFENDER，於 24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, 或請電: 40-21-206.34.70 or Fax: 40-21-264.17.99, E-mail 信箱: office@bitdefender.com.



序言

這份手冊提供給選擇 BitDefneder 網路安全 2009做為他們個人電腦上的安全解決方案。在這本書上的資訊不只是適合提供給電腦操作者使用，也適合任何一個可以在 Windows 環境下的使用者使用。

這本書將為您描述BitDefender網路安全 2009是由哪個公司及團隊所建立，並且引導您整個安裝的程序，教導您如何設定它。您將會知道如何去使用BitDefender網路安全 2009，如何去更新、測試及將它個人化。您將會學習到如何從 BitDefender 得到最好的服務。

我們希望您有一個愉快且有用的演講。

1. 本書的用法說明

1.1. 印刷上的常規

為了易於閱讀，此書使用了幾種文字的樣式。它們的外觀及意思描述在以下的表格裡面。

外觀	描述
sample syntax	語法樣本一起列印monospaced特性.
http://www.bitdefender.com	這個 URL 連結正指到其他外部的位置，http 或 ftp 伺服器。
support@bitdefender.com	在文字中插入聯絡的電子郵件位址資訊。
"序言" (p. xiv)	這是一個內部的連結，連結到這份手冊的其他位置。
filename	檔案及目錄使用monospaced 字型列印。
option	所有產品選項使用strong字元來列印。
sample code listing	程式的列表使用monospaced字元列印。

1.2. 警告

警告是以文字、圖表來標示，針對目前的段落，提醒您額外的資訊。


註
註解只是很短的意見。儘管您可以略過它，註解可以提供有價值的資訊，像是特定的功能或連結到一些相關的主題。


重要
這個要求您的注意並且建議不要跳過它。通常它提供非絕對重要但卻是有意義的資訊。


警告
這是極重要的資訊，您必須重視它。如果您依指示去做，將不會有壞的事發生。您應該仔細閱讀並了解它，因為它描述了極危險的事。

2. 本書的架構

本書包含幾個部份包含了幾個主題。 此外，有一個詞彙表讓您清楚一些技術的詞彙。

安裝. 逐步介紹安裝 BitDefender 在工作站。這是一個BitDefender網路安全 2009 詳細的安裝指導。透過這份指導，您可以成功地完成安裝程序。最後，當您需要反安裝 BitDefender 時，移除步驟也說明在其中。

基本管理. 基本管理及維護BitDefender。

進階管理. 一個關於BitDefender提供的防護能力的詳細介紹。 您會被指導如何調整及使用所有BitDefender模組更有效地保護您的電腦對抗所有惡意程式的威脅（病毒、間諜程式、病毒製造工具及其他)。

取得協助. 如果有一些未預期的情況發生，從何找尋及詢問，以取得協助。

BitDefender 救援光碟. BitDefender 救援光碟描述。它協助了解及使用這個可開機光碟所提供的功能。

詞彙表. 詞彙表能夠解釋您在本書上發現的一些技術專有名詞及罕見的項目說明。

3. 意見回饋

我們邀請您協助我們改進這份手冊。我們將盡全力測試及確認所有的資訊。當您發現在這份手冊中任何瑕疵，或者您認為該如何改進以提供給您最好的檔案，請寫下來告訴我們。



透過電子郵件寄到documentation@bitdefender.com讓我們知道。



重要
請用英文寫下您的所有檔案相關的電子郵件，我們可以更有效率地處理它們。



安裝

1. 系統要求

BitDefneder 網路安全 2009只能安裝在以下的作業系統中：

- Windows XP Service Pack 2 (32/64位元)或更高
- Windows Vista (32/64位元)或Windows Vista Service Pack 1
- Windows Home Server

在安裝之前，請確定您的電腦符合最低的硬體以及軟體要求。



註
要找出您所使用的作業系統版本以及硬體資訊，在桌面上的 我的電腦 點擊右鍵，然後選取 內容。

1.1. 硬體要求

使用Windows XP

- 800 MHz 或更快的處理器
- 256 MB 記憶體 (建議使用1 GB)
- 170MB 可用的硬碟空間(建議200MB)

使用Windows Vista

- 800 MHz 或更快的處理器
- 512 MB 記憶體 (建議使用 1 GB)
- 170MB 可用的硬碟空間(建議200MB)

使用Windows Home Server

- 800 MHz 或更快的處理器
- 512 MB 記憶體 (建議使用 1 GB)
- 170MB 可用的硬碟空間(建議200MB)

1.2. 軟體要求

- Internet Explorer 6.0 (或更高版本)

■.NET Framework 1.1 (可以在套件中安裝)

網路釣魚防護只能在這些地方使用：

■Internet Explorer 6.0 (或更高版本)
■Mozilla Firefox 2.0
■Yahoo! 即時通 8.1
■Windows Live (MSN) Messenger 8.5

即時通訊加密只能在這些地方使用：

■Yahoo! 即時通 8.1
■Windows Live (MSN) Messenger 8.5

反垃圾郵件防護適用於所有POP3/SMTP 電子郵件客戶端。 BitDefender 反垃圾郵件工具列整合在：

■Microsoft Outlook 2000 / 2002 / 2003 / 2007
■Microsoft Outlook Express
■Microsoft Windows Mail
■Thunderbird 1.5 and 2.0

2. 安裝BitDefender

找到安裝檔案並且點擊滑鼠兩下。它將開啟精靈，並引導您完成設定程序。

安裝精靈出現之前，BitDefender會檢查更新的安裝檔案。當有新的版本時，您將會被提示下載。您可以選擇點擊是以下載新的版本，或者點擊否繼續進行安裝步驟



安裝步驟



請依照以下步驟來安裝BitDefneder 網路安全 2009：

1. 點擊 下一步 繼續，或點擊 取消以離開安裝程序。
2. 點擊 下一步。

   如果您的電腦有安裝其他病毒防護軟體，BitDefneder 網路安全2009會警告您。點擊移除 以移除所有已安裝的元件。 如果您不要移除已刪除的產品，點擊 下一步繼續進行安裝。



警告

在安裝BitDefender之前，強烈建議您先移除其他的病毒防護軟體。同時使用兩個或以上的病毒防護軟體，會影響電腦系統的運作。

3. 請詳讀授權合約並點擊我同意。



重要

如果您不同意授權和約的內容，請點擊 取消。安裝程序將會中斷並結束。

4. 您可以選擇要安裝 BitDefender網路安全 2009的路徑。 預設的路徑是 C:\Program Files\BitDefender\BitDefender 2009。 如果您要變更安裝路徑，點擊瀏覽並選取您要安裝 BitDefender 病毒防護 2009 的目錄。。

   點擊 下一步。

5. 選取安裝程序的相關選項。 其中有些選項為預設：

   ■開啟讀我檔案 — 在軟體安裝結束後，開啟讀我檔案。

   ■在桌面建立一個捷徑 — 在軟體安裝結束後，在您的桌面上放一個 BitDefender 網路安全 2009的捷徑。

   ■安裝完成後退出CD - 在安裝完成後把CD退出；當您選擇用CD安裝時會出現此選項。

   ■關閉Windows防火牆 - 關閉Windows防火牆。



重要

因為BitDefender網路安全 2009已經包含一個先進的防火牆，我們建議您關閉Windows防火牆。 進行二個防火牆在同一台電腦可能引起問題。

   ■關閉Windows Defender - 把Windows Defender關閉；此選項只適用於Windows Vista。

點擊安裝 開始進行軟體的安裝。 如果您尚未安裝，BitDefender 會首先安裝.NET Framework 1.1。

請等待安裝程序完成。

6. 點擊 完成。 您的系統可能被要求重新啟動，令安裝精靈完成您的安裝程序。 我們建議您盡快重新啟動。



重要

在完成安裝並重新啟動之後，將會出現註冊精靈 以及 設置精靈。 完成這些精靈以註冊並設置BitDefender網路安全 2009並建立一個BitDefender 帳號。

如果您接受了預設的安裝路徑，您可以在Program Files看到一個新的資料夾BitDefender並包含子資料夾 BitDefender 2009。

2.1. 註冊精靈

完成安裝後第一次啟動電腦時，註冊精靈將會出現。 精靈將會幫助您註冊BitDefender並設置您的BitDefender 帳號。

您必須建立一個帳號以收到BitDefender更新檔案。 擁有BitDefender帳號，您可以享有免費的技術支援及特別的續購優惠。 如果您遺失了BitDefender授權序號，您可以透過http://myaccount.bitdefender.com並登入您的帳號以重新取得您的授權序號。



註

如果您不想使用這個精靈，點擊 取消。 您可以在任何時候執行註冊精靈，在使用者介面下方點擊註冊。

2.1.1. 步驟 1/2 - 註冊 BitDefneder 網路安全 2009



註冊

您可以檢視BitDefender 註冊狀態，現在使用的授權序號，以及授權序號將在幾天內到期。

希望繼續評估這個軟體，請選取繼續使用目前的序號。

註冊 BitDefneder 網路安全 2009：

1. 選取 我想要以新的序號註冊產品。
2. 在編輯欄位中輸入授權序號。



註
您可以在這些地方找到授權序號：
■光碟標籤。
■產品註冊卡。
■線上購買的電子郵件。



如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

點擊 下一步以繼續。

2.1.2. 步驟 2/2 — 建立一個 BitDefender 帳號



建立帳號

如果您不想建立 BitDefender 帳號，選取 跳過註冊並點擊完成。 否則，根據您目前的狀況選擇：

- "我沒有BitDefender 帳號" (p. 9)
- "我已經擁有BitDefender 帳號。" (p. 9)



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

我沒有BitDefender 帳號

選擇 建立新的 BitDefender 帳號 及提供所需的資料。 您在這裡所提供的資料將會被保密。

- E-mail address — 輸入您的電子郵件信箱。
- 密碼 — 為您的BitDefender帳號輸入一組密碼。 密碼長度至少要六個字元。
- 重複鍵入密碼 — 重新輸入先前的密碼。
- 名 — 輸入您的名字。
- 姓 — 輸入您的姓氏。
- "國家 —選擇您所在的國家。



註
在http://myaccount.bitdefender.com使用您提供的電子郵件地址和密碼來登入您的帳戶。

要成功建立一個帳號，您必須啟動您的電子郵件。確認您的電子郵件地址並依循 BitDefender 註冊服務所寄給您的電子郵件中的指示完成。

您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。選取一個選項：

- 傳送給我所有BitDefender的訊息
- 只傳送給我最重要的訊息
- 不要傳送任何訊息

點擊 完成。

我已經擁有BitDefender 帳號。

BitDefender 將會自動發現您先前電腦上登記的 BitDefender 帳號。 在這個情況下，請提供您的密碼。

如果您已經有一個帳戶,但是 BitDefender 並沒有偵測到，請選取登入到現有的 BitDefender 帳號並輸入您的電子郵件地址及密碼。

如果您忘記您的密碼，點擊 忘記您的密碼？ 並依循指示操作。

您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。選取一個選項：

■傳送給我所有BitDefender的訊息
■只傳送給我最重要的訊息
■不要傳送任何訊息

點擊 完成。

2.2. 設置精靈

在完成註冊精靈後，設置精靈將會出現。 精靈將會幫助您設置特定的產品模組，設定並執行重要的安全性任務。

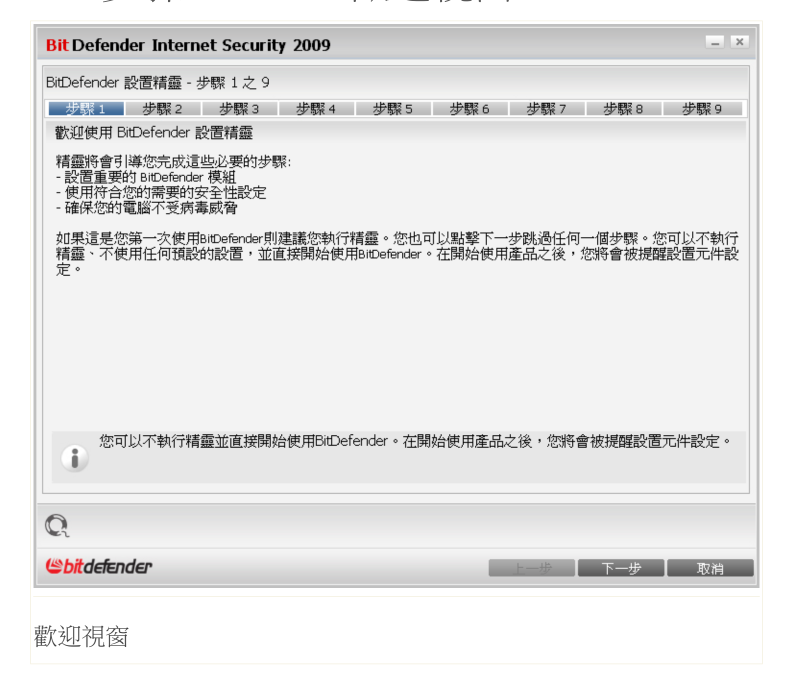
完成這個精靈並非強制的；然而，我們建議您如此做是為了節省時間並且確定您的系統在 網路安全 2009安裝前是安全的。



註

如果您不想使用這個精靈，點擊 取消。 BitDefender 在您開啟使用者介面時，將會提醒您需要設置的元件。

2.2.1. 步驟 1/9 — 歡迎視窗



歡迎視窗

點擊 下一步以繼續。

2.2.2. 步驟 2/9 — 選擇檢視模式。



檢視模式

根據您的BitDefender 使用經驗選取一個使用者介面檢視模式：

■基本檢視. 簡易的使用者介面，適合初學者或想要執行基本的任務並簡單解決問題的使用者。 您只要持續注意BitDefender 的警告與警示並修復出現的事件。

■進階檢視. 進階的使用者介面，適合熟悉的使用者以詳細設置產品設定。 您可以設置每一個元件並執行進階任務。

點擊 下一步以繼續。

2.2.3. 步驟 3/9 — 設置BitDefender網路

BitDefender Internet Security 2009

BitDefender 設置精靈 - 步驟 3 之 9

步驟 1 | 步驟 2 | 步驟 3 | 步驟 4 | 步驟 5 | 步驟 6 | 步驟 7 | 步驟 8 | 步驟 9

家庭管理設置

BitDefender 2009 includes a new component, Home Management, which enables you to create a virtual network of all the computers in your household and to manage all of the BitDefender products installed in this network. You can act as an administrator of a network that you create or you can be part of a network created and managed from another computer.

Click the check box below if you want to be part of the BitDefender Home Network. You will be required to enter a Home Management password which will allow the administrator of your network to control the BitDefender settings and actions on this computer remotely.

我想成爲家用網路中的一部分

家庭管理密碼：

重新輸入密碼：

要進一步了解BitDefender使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

bitdefender　上一步　下一步　取消

BitDefender網路設置

BitDefender　　讓您能夠在家中的電腦間建立一個虛擬網路，並管理網路中安裝的BitDefender　。

如果您要這台電腦成為BitDefender家庭網路的一部分，請依照以下步驟：

1. 選取 我要這台電腦成為BitDefender家庭網路的一部分。
2. 在編輯欄位中輸入相同的管理密碼。



重要

密碼能夠讓管理者從其他電腦管理這台電腦上的BitDefender　。

點擊 下一步以繼續。

2.2.4. 步驟 4/9 —設置身分管控

身分管控設置

身分管控能夠保護您在線上時免於被竊取敏感的資料。 根據您所建立的規則，身分管控將會掃描從網頁、電子郵件或即時通訊中有沒有出現特定字串(例如：信用卡號碼)。如果掃描到特定字串，該網頁、電子郵件或即時通訊將會被阻擋。

如果您想要使用身分管控，請依照以下步驟：

1. 選取我現在就要進行設置。
2. 建立規則以保護您的敏感資料。 要了解更多資訊，請參考 "建立身分管控規則" (p. 15)。
3. 如果有需要，在您所建立的規則中定義特定的例外。 要了解更多資訊，請參考"定義身分管控例外" (p. 16)。

點擊 下一步以繼續。

建立身分管控規則

要建立身分管控規則，點擊 加入。 設置視窗將會出現。



身分管控規則

您必須設定以下的參數：

■規則名稱 — 在編輯欄位中輸入規則的名稱。

■規則類型 — 選擇規則類型 (住址、姓名、信用卡號碼、身分證號碼等)。

■規則資料 —在編輯欄位中輸入您想要保護的資料。 舉例來說，如果您想保護您的信用卡號碼，在這裡輸入全部或部分的號碼。



註
如果您輸入少於三個字元，您將會被提示驗證資料。我們建議您最少三個字元以避免被阻擋錯誤發生。

您可以選擇在整個單字符合規則資料時套用規則，偵測到的字串事件相符時套用規則。

為了容易分辨規則所阻擋的資料，請在編輯方塊中提供詳細的規則描述。

選擇您希望 BitDefender 掃描的傳輸方式：

■掃描 HTTP — 掃描 HTTP(網站) 傳輸，並阻擋符合規則的外送資料。

■掃描 SMTP — 掃描 SMTP(電子郵件) 傳輸，並封鎖符合規則的外送電子郵件。

■掃描即時通訊 — 掃描即時通訊傳輸，並封鎖符合規則的外送即時訊息。

點擊 確定以加入規則。

定義身分管控例外

這是您可能須要對特定的身分規則定義例外的情況。 當您真的需要將您的信用卡資料藉由網路傳送遞交時，您可以設定規則的例外。

要管理例外規則，點擊 例外 。



身分管控例外

要加入例外，請依照下列步驟：

1. 點擊 加入按鈕以在表上新增項目。
2. 在指定允許的位址 點擊兩下，輸入您要加入例外的網址或是電子郵件地址。
3. 點擊兩下選擇類型並從選單選擇對應的您輸入的資料選項。
   ■如果您指定了一個網址，請選擇HTTP。
   ■如果您指定了一個電子郵件地址，請選擇SMTP。

要移除例外，選取並點擊 移除鈕。

點擊 確定 關閉視窗。

2.2.5. 步驟 5/9 —設置家長管控

家長管控設置

BitDefender 家長管控讓您能夠管控系統中每一個帳號存取網際網路以及特定應用程式。

如果您想使用家長管控，請依照以下步驟：

1. 我想使用家長管控
2. 在Windows 帳號的名稱上點擊右鍵並選取要套用的家長管控設定檔。

設定檔	描述
兒童	提供網站存取的限制，依據 14 歲以下使用者的建議設定值。 網頁中可能包含對幼童有害的內容(色情的、藥物的、暴力攻擊等) 都將被封鎖。

設定檔	描述
青少年	提供網站存取的限制，依據 14 到 18 歲使用者的建議設定值。 包含有色情或成人內容的網頁會被封鎖。
成年人	提供無限制的網站存取，不管網站的內容為何。



註

要針對特定帳號完整設置或停用家長管控，請開啟BitDefender 並切換至進階檢視選取家長管控。 您可以設置家長管控要阻擋的項目：

- 不適當內容的網路頁面。
- 在特定時間存取網際網路.(例如課業時間) 。
- 含有關鍵字的網頁及電子郵件將會被阻擋。
- 如遊戲、聊天、檔案分享程式或其他應用程式。
- 除了允許的聯絡人之外傳送的即時訊息。

點擊 下一步以繼續。

2.2.6. 步驟 6/9 —設置病毒報告



病毒報告選項

BitDefender 可以向BitDefender 實驗室傳送匿名的病毒報告，以持續追蹤病毒的散布。

您可以設置下列選項：

■寄送病毒報告 — 當您的電腦發現病毒時，寄發病毒報告到 BitDefender 實驗室。它將協助我們保持病毒疫情擴散的追蹤。

■啟動 BitDefender 疫情擴散偵測 — 將潛在病毒疫情擴散報告寄送到 BitDefender 實驗室。



註
這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。

點擊 下一步以繼續。

2.2.7. 步驟 7/9 —選取要執行的任務



選擇任務

為您的系統安全，設定網路安全 2009執行重要的防護任務。 以下的選項是可用的：

■更新 BitDefender 2009 引擎 (可能需要重新啟動) — 在下一個步驟，將更新 BitDefender 防毒標準版 2009 引擎，為了保護您的電腦免於最新的威脅。

■執行快速系統掃描 (可能需要重新啟動) — 在下一個步驟，快速系統掃描將被執行，允許 BitDefender 防毒標準版 2009 確認您的檔案在 Windows 及 Program Files 目錄不受到感染。

■在每天上午2:00 時執行全系統掃瞄 — 在每天上午2:00 時，執行全系統掃瞄。



重要

建議在進到下一個步驟之前您啟動這些選項以確保您的系統安全。

如果您只選擇最後一個選項，或者沒有選任何選項，您將跳過下一個步驟。

點擊 下一步以繼續。

2.2.8. 步驟 8/9 — 等待任務完成

任務狀態

等待任務完成。您可以看到在之前的步驟所選取的任務狀態。

點擊 下一步以繼續。

2.2.9. 步驟 9/9 —完成



完成

選擇 開啟我的 BitDefender 帳號 輸入您的 BitDefender 帳號。需要網際網路連線。

點擊 完成。

3. 升級

要將舊版本的BitDefender升及到BitDefender網路安全2009，請依照下列步驟。

1. 選用！ 若該版本的BitDefender包含反垃圾郵件，您可儲存 好友與垃圾郵件清單 以利升級程序結束後繼續使用。 要了解更多資料，請參閱說明檔案或是產品使用手冊。
2. 從您的電腦移除舊版的BitDefender。 要了解更多資料，請參閱說明檔案或是產品使用手冊。
3. 重新啟動電腦。
4. 請參照手冊的"安裝BitDefender" (p. 4) 頁面，安裝BitDefender 網路安全2009。

4. 修復或移除BitDefender

如果您想要修復或移除BitDefender 網路安全 2009，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2009 → 修復或移除。

您將被要求點擊 下一步去確認您的選擇。一個可讓您選擇的新視窗將會出現：

■修復 — 重新安裝先前設定時的所有程式元件。

如果您選擇修復BitDefender，將會出現一個新的視窗。 點擊修復以開始進行修復程序。

重新啟動電腦，然後點擊安裝以重新安裝 BitDefender 網路安全 2009。

當安裝程序完成，將會出現一個新的視窗。 點擊 完成。

■移除 — 移除所有已安裝的元件。



註
我們建議選擇移除當需要完全重新安裝元件。

如果您選擇了移除BitDefender，將會出現一個新視窗。



重要
當移除BitDefender時，您的系統不再免於惡意軟體的威脅，例如： 病毒、間諜程式。 如果您希望Windows的系統防護在移除BitDefender後開啟，請選擇對應的核取方塊。

點擊移除以開始從您的系統中移除BitDefender 網路安全 2009。

在移除過程中您會被提示給予我們一些意見 點擊 確定以進行我們一份不多於5條問題的問卷。 如果您並不希望填寫我們的問卷，點擊 取消。

當移除過程完成後，將會出現一個新的視窗。 點擊 完成。



註
移除程序完成後，我們建議您刪除位於 Program Files裡的 BitDefender 目錄。



移除BitDefender時發生錯誤

當移除BitDefender時發生錯誤時，移除程序會被終止，將會出現一個新視窗。 點擊 執行移除工具 以確保BitDefender從您的系統中完全移除。 移除工具會把所有在自動移除程序中不能移除的檔案及登錄鍵移除。

基本管理

5. 開始使用

只要您安裝BitDefender ，您的電腦就會被保護。

5.1. 開啟BitDefender 網路安全 2009

第一個步驟啟動BitDefender 應用程式，得到最好的服務。

要進入BitDefender網路安全2009的主要介面，請依照下面路徑：開始 → 程式集 → BitDefender 2009 → BitDefender 網路安全 2009 或者點擊兩下系統列上的BitDefender 圖示。

5.2. 使用者介面檢視模式

BitDefender網路安全2009可能會有初學者或者相當熟悉軟體的使用者。所以我們設計了兩種使用者介面以對應不同的使用者。

根據您對本產品的使用經驗，您可以選擇使用基本模式或是進階模式檢視BitDefender。



註
您可以點擊切換至基本檢視鈕或切換至進階檢視鈕，選擇使用其中一種視窗。

5.2.1. 基本檢視

基本檢視提供較簡易的介面，讓您以基本層級存取所有模組。您必須追蹤警告、嚴重警示，並修復不受歡迎的事件。



基本檢視

■您可以注意到，視窗的上方有兩個按鈕和一個狀態列。

項目	描述
設定	開啟視窗讓您能簡單地啟用或停用重要的安全模組(例如：防火牆、匿蹤模式、自動更新、遊戲模式等等)。
切換至進階檢視	開啟進階檢視視窗。您可以查看完整的模組清單、詳細的設置元件。在您下次進入使用者介面時，BitDefender 將記住此選項。
狀態	包含幫助您修復電腦安全弱點的資訊。

■在視窗中央有五個標籤。

標籤	描述
狀態顯示表	顯示有意義的產品統計數字及您的註冊狀態，以及重要手動任務的連結。

標籤	描述
安全防護	顯示安全防護模組的運行狀態(病毒防禦、反網路釣魚、防火牆、反垃圾郵件、即時通訊加密、隱私權、系統弱點檢查及更新模組)以及進行病毒、更新、系統弱點的檢查連結。
家長	顯示能讓您限制孩子存取網際網路及特定應用程式的模組狀態。
檔案管理員	顯示檔案保險箱的狀態及連至檔案保險箱的連結。
網路	顯示BitDefender 家庭網路結構。

■此外，BitDefender基本檢視視窗還包含了數個有用的捷徑。

連結	描述
我的帳戶	提供您建立或登入您的BitDefender帳戶。BitDefender帳戶提供您免費的線上支援。
註冊	提供您輸入新的授權序號，或檢視目前的授權序號及註冊狀態。
說明	進入說明文件，教您如何使用BitDefender。
支援	提供您連結至BitDefender支援小組。
歷史	提供您查看BitDefender在您的系統進行的所有任務的詳細歷史。

5.2.2. 進階檢視

進階檢視讓您可以存取每一個BitDefender產品元件。您可以設置進階設定以及追蹤進階功能。



進階檢視

■您可以注意到，視窗的上方有一個按鈕和一個狀態列。

項目	描述
切換至基本檢視	開啟基本檢視視窗。您可以在這裡查看基本的BitDefender介面，包括主要模組(安全、調整、檔案管理員、網路)以及狀態顯示表。在您下次進入使用者介面時，BitDefender 將記住此選項。
狀態	包含幫助您修復電腦安全弱點的資訊。

■在視窗的左端有一個選單，包含所有的安全模組。

模組	描述
一般	提供您存取一般設定，或檢視狀態顯示表和詳細的系統資訊。
病毒防護	提供您詳細設置您的病毒防禦及掃描操作，設定例外及設置隔離區模組。
反垃圾郵件	讓您能夠保持您的收件夾沒有垃圾郵件並詳細設置反垃圾郵件設定。
防火牆	讓您保護電腦免於內送及外送的未授權連線威脅。它就像是進出口的警衛 — 它會保持注意您的網際網路連線，並追蹤誰可以存取網際網路，誰被阻擋存取。
隱私權管控	在您使用網路時預防資料竊取並保護您的隱私。
家長管控	讓您可以利用自訂的電腦存取規則，保護您的兒童遠離不正當的網頁內容。
加密	讓您可以加密Yahoo and Windows Live (MSN) Messenger 的通訊並同時將本地的重要檔案、資料夾和磁碟分割加密。
弱點檢查	提供您保持電腦中重要軟體的更新。
遊戲/筆電模式	當您使用電池運作電腦時，提供您延緩BitDefender排定的任務，在您玩遊戲時忽略警示及彈出式視窗。
網路	提供您設置與管理您家庭網路中的電腦。
更新	提供您獲得最近更新的資訊，更新產品與設置更新程序。
註冊	讓您可以註冊BitDefender網路安全2009、更改授權序號或建立BitDefender帳號，點擊 註冊 連接，位於 BitDefender 安全防護中心視窗的上面。

■此外，BitDefender進階檢視視窗中包含了數個有用的捷徑。

連結	描述
我的帳戶	提供您建立或登入您的BitDefender帳戶。BitDefender帳戶提供您免費的線上支援。
註冊	提供您輸入新的授權序號，或檢視目前的授權序號及註冊狀態。
說明	進入說明文件，教您如何使用BitDefender。

連結	描述
支援	提供您連結至BitDefender支援小組。
歷史	提供您查看BitDefender在您的系統進行的所有任務的詳細歷史。

5.3. 系統工具列的BitDefender圖示

為了更快速的管理整個程式，您也可以使用系統工具列的BitDefender圖示。

如果您連點這個圖示將開啟BitDefender。您也可以按下滑鼠右鍵，將出現一個右鍵選單，提供 BitDefender 的快速管理。



BitDefender圖示

顯示 - 開啟BitDefender。

- 協助 —開啟詳細說明BitDefender 網路安全2009的檔案。
- 關於 - 開啟 BitDefender 網頁。
- 修復所有事件 - 幫助您移除安全弱點。
- 開 / 關遊戲模式 -遊戲模式 開 / 關。
- 立即更新 - 立刻執行更新。 您可以在新開啟的視窗檢視更新狀況。
- 基本設定 - 提供您啟動或停用重要的安全模組。 您可以在新開啟的視窗點擊選擇啟用/不啟用。

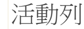
當遊戲模式啟動時，您可以看見英文字母G顯示在 BitDefender圖示上。

若發生危害您系統安全的嚴重事件時，一個驚嘆號將會出現在 BitDefender圖示上。您可以將滑鼠游標移至圖示以檢視危害您系統安全事件的數量。

5.4. 掃描活動列

這個 掃描活動列 是您的系統上掃描活動的圖形。




活動列

灰色線條(檔案區)顯示每秒掃描的檔案數量，從0到50的範圍。

在網路區的橘色線條顯示已從網路每秒掃描的檔案，從 0 到 100 的大小。



註
這個掃描活動列將利用紅色交叉線在相對應的 (檔案區 或 網路區) 空間裡通知您，當防毒機制已關閉時。這種方式使您不用開啟管理主控台即可得知是否被保護。

您可以使用掃描活動列來掃瞄目標。將您想掃描的目標拖曳至掃描活動列即可。 請參閱"拖放掃描" (p. 147)，以獲得更多資訊。

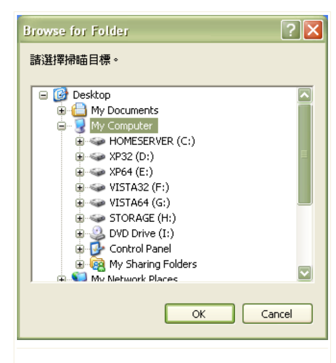
當您不想再看到這個即時的圖形顯示，請按下滑鼠右鍵，並選擇隱藏。 要完全隱藏這個視窗，請依照這些步驟：

1. 點擊切換至進階檢視 (如果您正在 基本檢視)。
2. 從左側選單中點擊 一般 模組。
3. 點擊 設定 標籤。
4. 取消選取啟動掃描活動列 (螢幕上顯示產品活動) 方塊。

5.5. BitDefender 手動掃瞄

如果您想快速掃瞄某個資料夾，可以使用 BitDefender 手動掃瞄。

如果您想執行BitDefender手動掃瞄，請依照Windows 開始程式集的路徑： 開始 → 程式集 → BitDefender 2009 → BitDefender 手動掃描 以下視窗將會顯示：



BitDefender 手動掃瞄

請瀏覽，選擇要掃瞄的資料夾並按下 確定。 BitDefender 掃瞄器會出現並引導您完成整個掃瞄過程。

5.6. 遊戲模式

創新的遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。 當您啟動遊戲模式，下列設定將會被套用：

- 使處理程序時間和記憶體消耗降到最低
- 延緩自動更新和自動掃描
- 消除所有警示和彈出式視窗
- 只掃描最重要的檔案

當遊戲模式啟動時，您可以看見英文字母G顯示在 BitDefender圖示上。

5.6.1. 執行遊戲模式

可以選擇下列其中一種方式啟動遊戲模式：

- 在系統工具列按下滑鼠右鍵點擊 BitDefender 圖示，並選擇 啟動遊戲模式。
- 同時按下 Ctrl+Shift+Alt+G 鍵(預設熱鍵)。



重要
請記得在您遊戲結束時關閉遊戲模式。只要重複執行開啟的方式，即可關閉。

5.6.2. 變更遊戲模式熱鍵

如您想更改快速鍵，請按照以下步驟：

1. 點擊切換至進階檢視 (如果您正在 基本檢視)。
2. 於左側選單點擊 遊戲/筆電模式。
3. 點擊遊戲模式標籤。
4. 點擊進階設定鈕。
5. 在使用熱鍵選項，設定您要的熱鍵：
   - 您可以按下：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)以選擇使用它們當做熱鍵。
   - 在編輯欄鍵入字母以對應熱鍵。

舉例而言，如果您想要用Ctrl+Alt+D當作熱鍵，您必須按下Ctrl與Alt並且輸入D。



註
取消選取使用熱鍵就可以停用熱鍵。

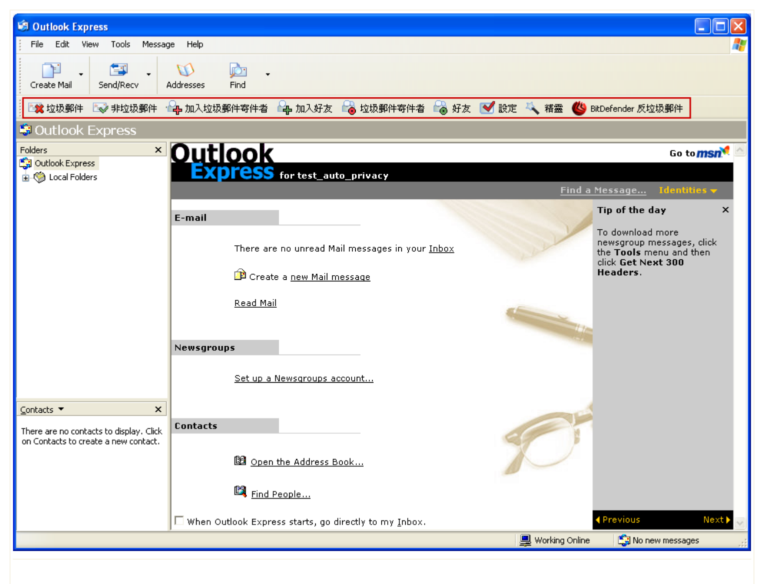
5.7. 整合進入客戶郵件內

BitDefender透過一個直覺且易於使用的工具列，直接與下列的電子郵件客戶端整合：

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

5.7.1. 反垃圾郵件工具列

您能看到反垃圾郵件工具列在電子郵件客戶端上方。



反垃圾郵件工具列



重要

BitDefender 反垃圾郵件功能在 Microsoft Outlook 或 Outlook Express 有不同之處，在 Microsoft Outlook 垃圾郵件會被移到 垃圾郵件資料夾，而在 Outlook Express 裡，垃圾郵件會被移到 刪除的郵件 資料夾。二者的垃圾郵件都會在主旨標示 SPAM。

在 Microsoft Outlook 裡，垃圾郵件 資料夾會自動由 BitDefender所建立，並與其他 資料夾清單(日曆、聯絡人等) 列於相同層級。

在 BitDefender 工具列的每個按鈕都將在下面進行解釋：

- 垃圾郵件 — 送一個訊息到Bayesian模組指出所選擇的電子郵件為垃圾郵件。這個電子郵件將被標示為垃圾郵件並移到 垃圾郵件資料夾。

  未來的電子郵件若符合相同的模式，都將被標示為垃圾郵件。



註

您可以選取一個或多個您想要的電子郵件。

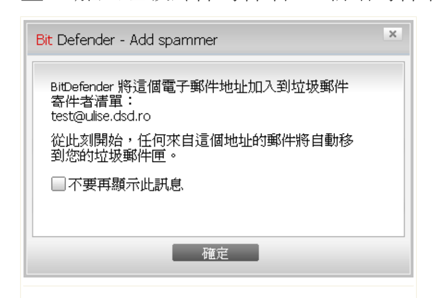
-  非垃圾郵件 — 傳送一個訊息到Bayesian模組指出所選的電子郵件不是垃圾郵件，不應該被標示為垃圾郵件。這個電子郵件將從 垃圾郵件 資料夾移到 收件匣。

  未來的電子郵件若符合相同的模式，都將不會被標示為垃圾郵件。

  註
  您可以選取一個或多個您想要的電子郵件。

  重要
  非垃圾郵件 按鈕會在您選擇一個郵件為 垃圾郵件時而啟動 (一般來說這些郵件是放在 垃圾郵件資料夾)。

-  加入垃圾郵件寄件者 —新增寄件者到 垃圾郵件寄件者清單。



加入垃圾郵件寄件者

選擇 不要再顯示這個訊息 當您新增一個垃圾郵件寄件者位址到這個清單時，您不想要再次被提示。

點擊 確定 關閉視窗。

未來從這個位址寄來的電子郵件都將被標示為垃圾郵件。

註
您可以選取一個或多個您想要的寄件者。

-  加入好友 —新增寄件者到 好友清單。



加入好友

選擇 不要再顯示這個訊息 當您新增一個好友的位址到這個清單時，您不想要再次被提示。

點擊 確定 關閉視窗。

您將會收到來自這個位址的電子郵件，不管它們的內容為何。



註
您可以選取一個或多個您想要的寄件者。

■ 垃圾郵件寄件者－開啟垃圾郵件寄件者清單是一個電子郵件位址清單，它包含您不想接受到的郵件，不管它的內容為何。



註
任何來自 垃圾郵件寄件者清單 的電子郵件，都將自動地被標示為垃圾郵件，不需要進行處理。



垃圾郵件寄件者清單

在這裡您可以從 垃圾郵件寄信者清單 加入或刪除內容。

如果您想要新增一個電子郵件位址，勾選 電子郵件位址 選項，輸入位址並點擊 按鈕。則位址將會出現在 垃圾郵件寄件者清單。



重要

語法：name@domain.com。

如果您想要新增一個網域，勾選 網域名稱 選項，輸入網域並點擊 按鈕。則網域將會出現在 垃圾郵件寄件者清單。



重要

語法：

- @domain.com、*domain.com 及 domain.com — 所有從 domain.com 接收到的電子郵件都將被標示為垃圾郵件；
- *domain* — 所有從 domain (不管網域的字尾為何) 接收到的電子郵件都將被標示為垃圾郵件；
- *com — 所有接收到以 com 為網域字尾的電子郵件都將被標示為垃圾郵件。

從輸入電子郵件帳號從 匯入電子郵件位址 由下拉式選單選擇 Windows 通訊錄/Outlook Express 資料夾 匯入電子郵件位址 Microsoft Outlook/Outlook Express。/ Windows Mail 選擇適當的選擇從進入電子郵件地址從 跳出的選擇單。

Microsoft Outlook Express 將出現一個新的視窗，您可以選擇您想要加入 垃圾郵件寄件者清單 的資料夾。選取他們並點擊 選擇。

二者的電子郵件位址都將會出現在匯入清單，選擇需要的並點擊 增加它們到 垃圾郵件寄件者清單。如果您點擊 所有電子郵件位址將新增到這個清單。

要刪除清單中的一個項目，選擇它並點擊 移除 按鈕。如果您點擊 清除清單 按鈕，您將刪除清單中所有的內容，請注意：刪除後不可能再回復它。

使用 儲存/ 載入按鈕去儲存/載入 垃圾郵件寄件者清單到需求的位址。這個檔案將以 .bwl 為副檔名。

當您載入一個先前儲存的清單，選擇 當載入時，清空目前的清單，則目前的清單即會被重新清除。

點擊 套用及 確定以儲存並關閉 垃圾郵件寄件者清單。

- 好友－開啟好友清單是一個電子郵件位址清單，它包含您想接受到的郵件，不管它的內容為何。



註
任何列於 好友清單 的電子郵件，都會自動地傳送到您的收件匣而不需進行處理。



好友清單

在這裡，您可以從 好友清單 加入或刪除內容。

如果您想要新增一個電子郵件位址，勾選 電子郵件位址 選項，輸入位址並點擊 ⊡ 按鈕。電子郵件位址將出現在 好友清單。



重要

語法：name@domain.com。

如果您想要新增一個網域，勾選 網域名稱 選項，輸入網域並點擊 ⊡ 按鈕。網域名稱將會出現在 好友清單。



重要

語法：

- @domain.com、*domain.com 及 domain.com — 所有從 domain.com 接收到的電子郵件訊息都將直接傳到您的 收件匣 不管它們的內容為何；
- *domain* — 所有從 domain(不管網域的語法) 接收到的電子郵件訊息都將直接傳到您的 收件匣 不管它們的內容為何；
- *com — 所有接收到的電子郵件以 com 為字尾，都將直接傳送到您的 收件匣 不管它們的內容為何；

從輸入電子郵件帳號從　匯入電子郵件位址　由下拉式選單選擇　Windows　通訊錄/Outlook　Express　資料夾　匯入電子郵件位址　Microsoft　Outlook/Outlook　Express。/ Windows Mail 選擇適當的選擇從進入電子郵件地址從 跳出的選擇單。

Microsoft Outlook Express 將出現一個新的視窗，您可以選擇您想要加入 好友清單　的資料夾。選取他們並點擊 選擇。

二者的電子郵件位址都將會出現在匯入清單，選擇需要的並點擊 增加它們到 好友清單。如果您點擊 所有電子郵件位址將新增到這個清單。

要刪除清單中的一個項目，選擇它並點擊 移除 按鈕。如果您點擊 清除清單 按鈕，您將刪除清單中所有的內容，請注意：刪除後不可能再回復它。

使用　儲存/　載入　按鈕去儲存/載入　好友清單　到需要的位置。這個檔案以 .bwl 為副檔名。

當您載入一個先前儲存的清單，選擇 當載入時，清空目前的清單，則目前的清單即會被重新清除。



註

我們建議您可以將好友的名稱及電子郵件位址加入好友清單。BitDefender 不會阻擋來自這些清單的郵件，因此，增加好友清單會更可以確定正常的信件可以存取。

點擊 套用 及 確定以儲存並關閉 好友清單。

- 設定－開啟設定視窗以讓您設置有關反垃圾郵件模組的設定



設定

以下的選項是可用的：

- 移動郵件到刪除的項目 — 移動垃圾郵件到 刪除的項目 (只有 Microsoft Outlook Express)；
- 標示郵件為 '已讀取' — 標示所有垃圾郵件為已讀取，當新的垃圾郵件寄到時，不讓使用者受到打擾。

如果您的反垃圾郵件過濾器是非常不準確的，您也許需要清除過濾器資料庫，並且重新訓練 Bayesian過濾器。點擊 清除反垃圾郵件資料庫 重新設定 Bayesian過濾器。

使用 儲存 Bayes/ 載入 Bayes 按鈕，進行儲存 / 載入 Bayesian資料庫 清單在需要的位置。這個檔案將以 .dat 為副檔名。

點擊警示標籤以存取能讓您停用確認視窗的頁面 加入垃圾郵件寄件者 and 加入好友按鈕。



註
在 警示 您也可能/ 不可能在視窗出現請選擇電子郵件信息警告。當您選擇一個組合而非電子郵件訊息的時候，這警告會出現。

- 精靈 — 打開 精靈 它將協助您進行訓練 Bayesian過濾器，以讓BitDefender 反垃圾郵件的效率將增加。您也可以從您的 通訊錄 增加電子郵件到 好友清單 / 垃圾郵件寄件者清單。
- BitDefender 反垃圾郵件 — 打開 BitDefender 使用者介面。

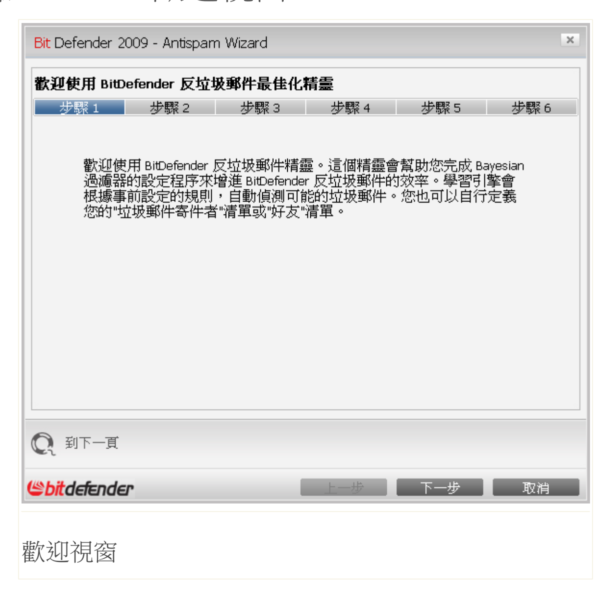
5.7.2. 反垃圾郵件設置精靈

在安裝完 BitDefender 第一次啟動 Microsoft Outlook / Outlook Express，精靈將會出現，並協助您設定 好友清單 及 垃圾郵件寄件者清單 並訓練 Bayesian過濾器 以加強反垃圾郵件過濾器的效率。



註
您可以在任何您想要的時間啟動精靈，從 反垃圾郵件工具列 點擊 精靈 按鈕。

步驟 1/6 — 歡迎視窗



歡迎視窗

點擊 下一步。

步驟 2/6 — 填入好友清單

填入好友清單

在這裡您可以檢視所有在您的 通訊錄 中的電子郵件。請選擇要加入您 好友清單 的電子郵件(我們建議您選擇全部)。您將收到所有來自這些位址的電子郵件，不管它們的內容為何。

把您所有連絡人加入好友清單，按選擇全部。

選擇 跳過這個步驟 如果您想要略過這個步驟。點擊 返回 到前一個步驟或點擊 下一步 繼續設定精靈。

步驟 3/6 — 刪除Bayesian資料庫



刪除Bayesian資料庫

您可能發現您的垃圾郵件過濾器開始失去效率。這可能是由於不正確的訓練 (如：您誤將正常的信件標示為垃圾郵件，或者相反)。如果您的過濾器非常不正確，您可能需要清除過濾器資料庫，並依照以下步驟重新訓練過濾器。

選擇 清除反垃圾郵件過濾器資料庫 如果您想要重設Bayesian資料庫。

使用 儲存 Bayes/ 載入 Bayes 按鈕去儲存 / 載入 Bayesian資料庫 到需要的位置。這個檔案是以 .dat 為副檔名。

選擇 跳過這個步驟 如果您想要略過這個步驟。點擊 返回 到前一個步驟或點擊 下一步 繼續設定精靈。

步驟 4/6 — 透過正常的郵件訓練Bayesian過濾器。



透過正常的郵件訓練Bayesian過濾器

請選擇一個包含正常電子郵件的信件匣。這些郵件將被使用來訓練反垃圾郵件過濾器。這裡有兩個進階選項的選擇在目錄清單：

■包含子目錄 — 包含您所選擇子目錄。
■自動加入到好友清單 — 自動加入寄件者到 好友清單。

選擇 跳過這個步驟 如果您想要略過這個步驟。點擊 返回 到前一個步驟或點擊 下一步 繼續設定精靈。

步驟 5/6 — 透過垃圾郵件訓練Bayesian過濾器



透過垃圾郵件訓練Bayesian過濾器

請選擇一個含有垃圾郵件的信件匣。這些郵件將使用來訓練反垃圾郵件過濾器。



重要
請確認您所選擇的信件匣並沒有包含正常信件，否則反垃圾郵件的效率將會降低。

這裡有兩個進階選項的選擇在目錄清單：

■包含子目錄 — 包含您所選擇子目錄。
■自動加入到垃圾郵件寄件者清單 — 自動地加入寄件者到 垃圾郵件寄件者清單。

選擇 跳過這個步驟 如果您想要略過這個步驟。點擊 返回 到前一個步驟或點擊 下一步 繼續設定精靈。

步驟 6/6 — 總結



總結

在這裡您可以檢視設定精靈的所有設定，如果您想做任何設定的修改，仍可回到先前的步驟。(點擊 返回)。

如果您不想做任何更改，點擊 完成 離開這個精靈。

5.8. 整合入網頁瀏覽器

BitDefender能夠防護您的電腦免於網路釣魚的威脅。 它能夠掃描您正在瀏覽的網站，並警告您有網路釣魚的威脅。 您可以設定網站白名單，如此BitDefender將不會掃描這些網站。

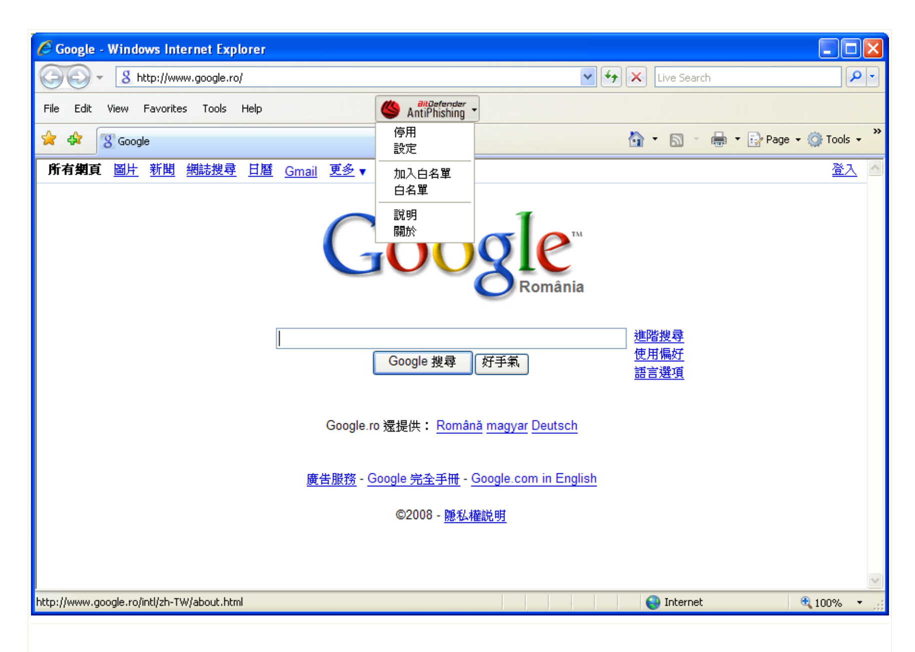
BitDefender 將功能整合，透過一個直覺且易於使用的工具列進入下列瀏覽器：

- Internet Explorer
- Mozilla Firefox

您可以輕易的使用整合入上列瀏覽器的BitDefender反網路釣魚工具列，管理反網路釣魚防護功能及白名單。

反網路釣魚工具列位於Internet Explorer 的上方，以 BitDefender圖示表示。 要開啟工具列選單，請點擊這裡。

註
如果您無法看見工具列，開啟 檢視 選單，選擇工具列並選取BitDefender 工具列。



反網路釣魚工具列

在工具列選單會有以下可用的命令：

■啟動 / 停用 - 啟動 / 停用 BitDefender反網路釣魚工作列。



註
如果停用反網路釣魚工作列，您將不再受反網路釣魚的保護。

■設定 - 開啟一個視窗，您可以調整反網路釣魚工作列的設定。

以下的選項是可用的：

・啟動掃描 - 啟動反網路釣魚掃描。
・加入白名單前先詢問 - 在您將網站加入白名單前，先詢問您。

■加入白名單 - 將目前的網站加入白名單。



註
將網站加入白名單意謂著BitDefender將不會再針對該網站使用反網路釣魚功能。建議您只將您絕對信任的網站加入。

■檢視白名單 - 開啟以檢視白名單。

您可以查看所有不會被BitDefender反網路釣魚引擎掃描的網站。

如果您要從白名單中移除任何網站使您可以得知此網站是否有網路釣魚威脅，點擊旁邊的移除按鈕。

您可以將您絕對信任的網站加入白名單，如此這些網站將不會再被反網路釣魚引擎掃描。 要將網站加入白名單，在所對應的欄位輸入網站的網址並點擊加入。

■說明 - 開啟一個說明檔。

■關於 - 開啟一個視窗，在此您可以得到更多關於BitDefender的資訊，並尋求相關協助。

5.9. 整合進入即時通訊

BitDefender提供加密功能，防護您的機密文件和您透過Yahoo即時通與MSN Messenger的即時交談對話。

BitDefender加密所有您的即時交談訊息，預設規定：

■您的交談對象已安裝了支援即時通訊加密的BitDefender版本，並且即時通訊加密在您的即時通訊程式上已經啟動。

■您和您的交談對象使用Yahoo即時通或是Windows Live (MSN) Messenger交談。



重要
若您的交談對象使用，如Meebo、或其他支援Yahoo即時通與Windows Live (MSN) Messenger的網頁型的交談程式，BitDefender將無法加密對話。

您可以從交談視窗中使用BitDefender工具列，輕易的設置即時通訊加密。

在BitDefender工具列點擊右鍵，將提供您下列的選項：

■對某位交談對象永久啟動 / 停用加密。



■邀請某位交談對象使用加密。

■從家長管控黑名單中移除某位交談對象。

對istrate_ciprian永久停用加密
邀請istrate_ciprian使用加密
加入istrate_ciprian至家長管控黑名單

即時通訊加密選項

點擊上述選項就可以使用其功能。

6. 狀態顯示表

點擊狀態顯示表標籤，您可以看到產品的統計數字、您的註冊狀態，以及最重要的手動任務連結。



狀態顯示表

6.1. 概觀檢視

這裡您可以查看關於更新、帳戶、註冊狀態及授權序號資訊的統計資料概況。

項目	描述
上次更新	顯示您上次更新產品的日期。請定期更新以完整保護您的系統。
我的帳戶	顯示用來存取線上帳戶的電子郵件地址，您可以使用它存取您的線上帳戶以重新取得您遺失的BitDefender授權序號、得到BitDefender支援及其他服務。

項目	描述
註冊。	顯示您的授權序號及狀態。若您的序號已過期，請續購或升級產品以保護您的系統安全。
到期	顯示授權序號到期的天數。

從任務頁面點擊立即更新鈕即可更新BitDefender。

要新建或登入您的BitDefender帳戶，請依照以下步驟。

1. 點擊視窗下端的我的帳戶，將開啟網頁。
2. 輸入您的使用者名稱以及密碼，並點擊登入鈕。
3. 若您想新建一個BitDefender帳戶，選擇您還沒有帳戶嗎？並輸入要求的資訊。


註
您在這裡所提供的資料將會被保密。

要註冊BitDefender網路安全2009，請依照下列步驟。

1. 點擊視窗下端的我的帳戶，將開啟一個逐步註冊精靈。
2. 點擊我想以新序號註冊產品鈕。
3. 在對應的文字框中輸入新的授權序號。
4. 點擊 完成。

要購買新的授權序號，請依照以下步驟。

1. 點擊視窗下端的我的帳戶，將開啟一個逐步註冊精靈。
2. 點擊續購您的BitDefender授權序號連結，將開啟網頁。
3. 點擊立即購買鈕。

6.2. 任務

這裡您可以找到最重要的安全任務連結：全系統掃描、深度掃描、立即更新。

以下的按鍵是可用的：

- 全系統掃描 - 執行一個完整的系統掃描(除了資料封存)。
- 深度掃瞄 - 執行針對您電腦系統的完整掃瞄(包含資料封存)。
- 立即更新 - 立刻執行更新。

6.2.1. 使用BitDefender掃瞄

要掃描您電腦中的惡意程式，請點擊對應按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述：

任務	描述
全系統掃瞄	掃描整個系統，資料封存除外。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
深度掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。



註

由於深度掃瞄與全系統掃瞄　是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，或在您的系統閒置時執行。

當您執行掃描程序時，BitDefender掃描器會立刻出現。

依照三步驟指引執行掃描任務。

6.2.2. 更新 BitDefender

每天都有新的惡意程式被發現及識別，所以保持最新的BitDefender病毒特徵碼非常重要。

當您啟動您的電腦系統時，BitDefender已預設檢查是否有更新，之後每小時都會持續的檢查更新。 如果您想更新BitDefender，點擊立即更新鈕。 更新程序會立即啟動並且出現下列視窗：

Bit Defender Internet Security 2009

更新

步驟 1

BitDefender 更新

BitDefender 將會自動檢查並運行新的更新檔案。運行更新之前，請確認您已連線到網路。

狀態:　更新檢查中

檔案：　0 %　0 kb

全部的更新：　0 %　0 kb

要進一步了解BitDefender使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

bitdefender　完成　取消

更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序表示檔案會漸進地更新替換。如此更新程序不會影響產品性能，同時所有的弱點將被排除。

如果您想要關閉此視窗，請點擊取消。 然而，這並不會終止更新程序。



註

如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

如果需要，請重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。

點擊重新啟動以重新啟動您的電腦。

如果您想要稍後再重新啟動您的系統，請點擊好。 建議您盡快重新啟動您的系統。

7. 安全防護

BitDefender 的安全防護模組能夠協助您的電腦免受病毒威脅並且能夠隨時自動更新。

請點擊安全防護 標籤，進入安全防護模組。



安全防護

安全防護模組包含兩個頁面：

■受監控元件 - 您可以查看每一個安全模組的受監控元件完整清單。您可以選擇要監控哪一個模組，但建議您監控所有的元件。

■任務 - 您可以在這裡找到最重要的安全任務連結：全系統掃描、深度掃描及立即更新。

7.1. 受監控元件

受監控的元件被分成數個群組。

種類	描述
本機安全	在這裡您可以確認每一個安全模組的狀態。
線上安全	這裡您可以檢視每一個安全模組的狀態，當您在網際網路時保護您的電腦。
系統弱點掃瞄	您可以在這裡確認電腦中重要的軟體是否經過更新，並確認Windows帳戶密碼的安全性。

點擊 "+" 號方塊展開種類， "-" 號方塊關閉。

7.1.1. 本機安全

在任何問題出現可能影響您的電腦安全時，及時提醒您是非常重要的。藉由監控每個安全防護模組，BitDefender 網路安全2009不只在您的設定可能影響您的電腦安全時提醒您，如果您遺忘了重要的任務也會同時受到提醒。

關於本機安全的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
即時檔案防護已啟動	保證系統中所有您存取的檔案、或者應用程式執行的程式都已被掃描。
您今天已經掃瞄您電腦中的惡意程式	強烈建議您立即執行手動掃描，確認您電腦中的檔案是否不受惡意程式威脅。
自動更新已啟動	請維持自動更新啟動，確保惡意程式特徵碼是最新的狀態。
立即更新	產品及惡意程式特徵碼更新正在進行。
防火牆已啟動	保護您的電腦遠離惡意程式及駭客。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

7.1.2. 線上安全

關於線上安全的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
反垃圾郵件已啟動	確保您的電子郵件經過掃描沒有惡意程式，並過濾垃圾郵件。
身分管控已啟動	透過掃描網路及郵件傳輸中的特別字串，幫助您維護私密檔案的安全。建議您啟動身分管控以保護您的私密檔案(例如：電子郵件地址、使用者名稱、密碼、信用卡號碼)安全不被偷竊。
Firefox反網路釣魚保護已啟動	BitDefender能夠防護您的電腦免於網路釣魚的威脅。
Internet Explorer 反網路釣魚保護已啟動	BitDefender能夠防護您的電腦免於網路釣魚的威脅。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

7.1.3. 系統弱點掃瞄

關於系統弱點的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
系統弱點檢查已啟動	監控Microsoft Windows更新、Microsoft Office更新及Windows帳戶密碼，以確保您的作業系統經過更新、密碼安全。
重要的Microsoft更新	安裝可用的重要Microsoft更新。
其他Microsoft更新	安裝可用的次要Microsoft更新。

事件	描述
Windows自動更新已啟動	若有新的Windows安全性更新，立即安裝。
管理者 (安全的密碼)	顯示特定使用者密碼的強度。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

7.2. 任務

這裡您可以找到最重要的安全任務連結：全系統掃描、深度掃描、立即更新。

以下的按鍵是可用的：

- 全系統掃描 - 執行一個完整的系統掃描(除了資料封存)。
- 深度掃瞄 - 執行針對您電腦系統的完整掃瞄(包含資料封存)。
- 掃描我的文件 - 執行檔案資料夾的快速掃描。
- 立即更新 - 立刻執行更新。
- 系統弱點掃瞄

7.2.1. 使用BitDefender掃瞄

要掃描您電腦中的惡意程式，請點擊對應按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述：

任務	描述
全系統掃瞄	掃描整個系統，資料封存除外。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
深度掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。

任務	描述
掃描我的文件	利用這個任務掃描重要的使用者資料夾：我的文件，桌面和開始功能表。 這麼做可以保障您的檔案安全並且提供安全的環境運作應用程式。



註

由於深度掃瞄與全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，或在您的系統閒置時執行。

當您執行掃描程序時，BitDefender掃描器會立刻出現。 依照三步驟指引執行掃描任務。

7.2.2. 更新 BitDefender

每天都有新的惡意程式被發現及識別，所以保持最新的BitDefender病毒特徵碼非常重要。

當您啟動您的電腦系統時，BitDefender已預設檢查是否有更新，之後每小時都會持續的檢查更新。 如果您想更新BitDefender，點擊立即更新鈕。 更新程序會立即啟動並且出現下列視窗：

BitDefender Internet Security 2009

更新

步驟 1

BitDefender 更新

BItDefender 將會自動檢查並運行新的更新檔案。運行更新之前，請確認您已連線到網路。

狀態: 更新檢查中

檔案： 0 % 0 kb

全部的更新： 0 % 0 kb

要進一步了解BitDefender使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

bitdefender 完成 取消

更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序表示檔案會漸進地更新替換。如此更新程序不會影響產品性能，同時所有的弱點將被排除。

如果您想要關閉此視窗，請點擊取消。 然而，這並不會終止更新程序。



註

如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

如果需要，請重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。

點擊重新啟動以重新啟動您的電腦。

如果您想要稍後再重新啟動您的系統，請點擊好。 建議您盡快重新啟動您的系統。

7.2.3. 搜尋系統弱點

系統弱點掃描檢查Microsoft Windows更新、Microsoft Office更新及您的Windows 帳戶密碼，以確保您的作業系統經過更新、密碼安全。

要檢查您的電腦的弱點，請點擊系統弱點掃描並依照精靈的步驟進行。

步驟 1/6 - 選擇要檢查的系統弱點



系統弱點

點擊下一步以檢查系統已選的弱點。

步驟 2/6 – 系統弱點檢查



系統弱點檢查

等待BitDefender 完成系統弱點檢查。

步驟 3/6 – 更改不安全的密碼



使用者密碼

您可以檢視您電腦中的Windows使用者帳戶清單，以及他們的密碼防護層級。點擊修復以更改不安全的密碼。 一個新的視窗將會開啟。

BitDefender
Choose method to fix:
Force user to change password at next login
Change user password
Type password:
Confirm password:
OK Close

更改密碼

選擇修復此事件的方法：

- 強迫使用者在下次登入時更改密碼. BitDefender將提示使用者在下次登入Windows時更改密碼。
- 更改使用者密碼. 您必須在文字框輸入新的密碼。



註

使用大小寫混用、數字或特殊符號 (例如#、$或@)，以加強密碼。

點擊確定儲存密碼。

點擊 下一步。

步驟 4/6 - 更新應用程式



應用程式

您可以查看BitDefender檢查的的應用程式清單及他們的更新狀態。 若應用程式未更新，請點擊連結以更新到最新版本。

點擊 下一步。

步驟 5/6 - 更新Windows



Windows更新

您可以查看您尚未安裝的Windows更新清單。 點擊安裝所有系統更新以安裝所有可用的更新。

點擊 下一步。

步驟 6/6 - 檢視結果



結果

點擊關閉。



8. 家長

BitDefender 的家長模組能夠協助您的保持

要進入家長模組，點擊家長 標籤。



家長

家長模組包含兩個頁面：

- 受監控元件 - 您可以查看每一個安全模組的受監控元件完整清單。您可以選擇要監控哪一個模組，但建議您監控所有的元件。
- 任務 - 您可以在這裡找到最重要的安全任務連結：全系統掃描、深度掃描及立即更新。

8.1. 受監控元件

受監控元件包含以下：

種類	描述
家長管控	您可以在此檢查家長管控的狀態。家長管控能限制您的孩子存取網際網路或特定的應用程式。

點擊 "+" 號方塊展開種類， "-" 號方塊關閉。

8.1.1. 家長管控

家長管控監控能限制您的孩子存取網際網路或特定的應用程式的模組狀態。

關於家長管控模組的事件會描述的非常清楚。如果有任何可能影響您孩子的詞句，你將會看到一個紅色的狀態按鈕稱為修復。 或者顯示綠色的OK狀態鈕。

事件	描述
家長管控未設置	家長管控模組可以阻擋存取您認為不適當的網站，封鎖不當的網際網路存取時間(如：作功課時間)，封鎖遊戲、聊天、分享的應用程式等執行。

當狀態按鈕是綠色時，您的孩子可以安全的在網頁搜尋。要把按鈕變成綠色，請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

8.2. 任務

這裡您可以找到最重要的安全任務連結：全系統掃描、深度掃描、立即更新。

以下的按鍵是可用的：

■全系統掃描 - 執行一個完整的系統掃描(除了資料封存)。
■深度掃瞄 - 執行針對您電腦系統的完整掃瞄(包含資料封存)。
■立即更新 - 立刻執行更新。

8.2.1. 使用BitDefender掃瞄

要掃描您電腦中的惡意程式，請點擊對應按鈕執行特定的掃描任務。 您可以在下表檢視可用的掃描任務以及簡述：

任務	描述
全系統掃瞄	掃描整個系統，資料封存除外。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
深度掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。



註
由於深度掃瞄與全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，或在您的系統閒置時執行。

當您執行掃描程序時，BitDefender掃描器會立刻出現。

依照三步驟指引執行掃描任務。

8.2.2. 更新 BitDefender

每天都有新的惡意程式被發現及識別，所以保持最新的BitDefender病毒特徵碼非常重要。

當您啟動您的電腦系統時，BitDefender已預設檢查是否有更新，之後每小時都會持續的檢查更新。 如果您想更新BitDefender，點擊立即更新鈕。 更新程序會立即啟動並且出現下列視窗：



BitDefender Internet Security 2009

更新

步驟 1

BitDefender 更新

BitDefender 將會自動檢查並運行新的更新檔案。運行更新之前，請確認您已連線到網路。

狀態: 更新檢查中

檔案： 0 % 0 kb

全部的更新： 0 % 0 kb

要進一步了解BitDefender使用介面的各個選項，請將滑鼠移到該選項，即可顯示相對應的文字解釋。

bitdefender 完成 取消

更新 BitDefender

您可以在此視窗檢視更新狀態。

更新程序表示檔案會漸進地更新替換。如此更新程序不會影響產品性能，同時所有的弱點將被排除。

如果您想要關閉此視窗，請點擊取消。 然而，這並不會終止更新程序。



註

如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

如果需要，請重新啟動電腦。. 若有重大的更新，您將會被要求重新啟動您的電腦。

點擊重新啟動以重新啟動您的電腦。

如果您想要稍後再重新啟動您的系統，請點擊好。 建議您盡快重新啟動您的系統。



9. 檔案保險箱

BitDefender 的檔案保險箱模組能夠協助您保護您的檔案安全並維持私密性。要達成這個目標，請使用檔案保險箱。

檔案保險箱. 如果您想要保護您的私密檔案不受窺探。檔案管理員模組的檔案保險箱頁面能提供幫助。

■檔案保險箱是個針對個人資訊或私密檔案的安全儲存空間。

■檔案保險箱是個加密過的檔案，使用bvd為副檔名。

■當檔案加密後，資料將不會被竊取或被破解。

■當您掛載這個bvd檔案，一個新的磁碟機將會出現。有一個比較簡單的例子，掛載一個光碟映像檔案作為光碟使用。

只要打開我的電腦你就會看到您的檔案保險箱開啟為一個新的磁碟機，您可以執行任何的動作(複製、刪除、變更等等)。檔案在這個磁碟裡面的時候是安全的(因為掛載檔案時需要密碼)。 完成操作後，請將您的保險箱上鎖(卸載)以防護其內容。

要進入檔案管理員模組，點擊檔案保險箱 標籤。



檔案保險箱

■受監控的元件－讓您能夠檢視所有受監控元件的清單。您可以選取要監控的模組，建議您監控所有元件。

9.1. 受監控元件

受監控元件包含以下：

種類	描述
檔案保險箱	檔案保險箱是個針對個人資訊或私密檔案的安全儲存空間。它儲存於在您的電腦中。當檔案加密後，資料將不會被竊取或被破解。

點擊 "+" 號方塊展開種類， "-" 號方塊關閉。

9.1.1. 檔案保險箱

可能影響您的資料隱私權的事件會描述的非常清楚。如果有任何事物可能影響您的資料隱私權，你將會看到一個紅色的狀態按鈕稱為修復。 或者顯示綠色的OK狀態鈕。

事件	描述
檔案保險箱已啟動	檔案保險箱透過加密檔案來保護您的文件與資料。

當狀態按鈕是綠色時，您的資料安全危險已降到最低。要把按鈕變成綠色，請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

9.2. 任務

以下的按鍵是可用的：

- 加入檔案至保險箱－啟動精靈以讓您儲存重要私密的檔案、文件在一個已加密的保險箱磁碟中。
- 移除保險箱檔案 — 啟動精靈以讓您從檔案保險箱中刪除檔案。
- 檢視保險箱 —啟動精靈以讓您檢視您的檔案保險箱內容。
- 將保險箱上鎖 —啟動精靈以讓您將您的檔案保險箱上鎖並保護其內容。

9.2.1. 加入檔案至保險箱

檔案保險箱是個儲存有價值的資料的安全空間。檔案保險箱內的文件受到加密。

點擊加入檔案至保險箱精靈將會帶領您建立一個保險箱並加入文件在其中。

步驟 1/6 — 選擇目標

您可以在此選取要加入保險箱的檔案或資料夾。



目標

點擊 加入目標，選取要加入保險箱的檔案或資料夾並點擊 確定。 您所選擇的路徑將會出現在路徑欄位。 如果您要變更路徑，只要點擊旁邊的 移除鈕。



註
您可以選擇一個或數個位置：

點擊 下一步。

步驟 2/6 — 選取保險箱。

您可以在此建立新的保險箱，或選取一個原有的保險箱。



選取保險箱

如果您選取瀏覽以選取保險箱檔案， 您必須點擊瀏覽並選取檔案保險箱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟5，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟4。

如果您點擊選取原有的檔案保險箱， 您必須點擊想要的保險箱名稱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟5，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟4。

如果您原有的保險箱不符合您的需要，選取建立新的檔案保險箱，您將會跳至步驟3。

點擊 下一步。

步驟 3/6 —建立保險箱

您可以在此詳細說明新的保險箱資訊。



建立保險箱

要完成檔案保險箱相關資訊，請依照以下步驟：

1. 點擊 瀏覽並選取 bvd 檔案的位置。



註

請記得檔案保險箱是一個已加密的檔案，並以bvd為副檔名儲存於您的電腦中。

2. 從對應的下拉式選單中選取要指定給新的檔案保險箱的磁碟代號。



註

請記得當您掛載了bvd檔案，將會出現一個新的磁碟分割。

3. 在對應的欄位中輸入您的檔案保險箱密碼。



註

密碼長度至少要八個字元。

4. 重新輸入密碼。
5. 在對應的欄位中輸入數字以指定檔案保險箱的大小(MB)。



註
檔案大小應只包含數字。

點擊 下一步。

您將會跳到步驟5。

步驟4/6－密碼

您會在此被要求輸入選取的保險箱密碼。



輸入密碼

在對應的欄位中輸入密碼並點擊下一步。

步驟 5/6 — 總結

您可以在此回顧選取的操作。



總結

點擊 下一步。

步驟 6/6 —結果

您可以在此檢視保險箱內容。



結果

點擊 完成。

9.2.2. 從保險箱中移除檔案

點擊移除保險箱檔案，精靈將會帶領您完成從特定保險箱移除檔案的程序。

步驟 1/5 —選取保險箱

您可以在此指定要移除檔案的保險箱。



選取保險箱

如果您點擊瀏覽檔案保險箱，您必須點擊想要的保險箱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟3，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟2。

如果您點擊選取原有的檔案保險箱，您必須點擊想要的保險箱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟3，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟2。

點擊 下一步。

步驟 2/5 —密碼

您會在此被要求輸入選取的保險箱密碼。



輸入密碼

在對應的欄位中輸入密碼並點擊下一步。

步驟 3/5—選取檔案。

您可以在此檢視先前選取的保險箱檔案清單。



選取檔案

選擇您要移除的檔案並點擊下一步。

步驟 4/5 — 總結

您可以在此回顧選取的操作。



總結

點擊 下一步。

步驟 5/5 —結果

您可以在此檢視操作結果。



結果

點擊 完成。

9.2.3. 檢視保險箱中的檔案

點擊檢視保險箱，精靈將會帶領您檢視特定保險箱中的檔案。

步驟 1/4 —選取保險箱

您可以在此選取要瀏覽檔案的保險箱。



選取保險箱

如果您點擊瀏覽檔案保險箱，您必須點擊想要的保險箱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟3，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟2。

如果您點擊選取原有的檔案保險箱，您必須點擊想要的保險箱。您如果選取了一個已開啟(已掛載)的保險箱將會跳至步驟3，如果您選取了一個已上鎖(未掛載)的保險箱將會跳至步驟2。

點擊 下一步。

步驟 2/4 —密碼

您會在此被要求輸入選取的保險箱密碼。



輸入密碼

在對應的欄位中輸入密碼並點擊下一步。

步驟 3/4 — 總結

您可以在此回顧選取的操作。



總結

點擊 下一步。

步驟 4/4 —結果

您可以在此檢視保險箱中的檔案。



結果

點擊 完成。

9.2.4. 將保險箱上鎖

就像您已經知道的，檔案保險箱是一個已加密的bvd檔案。檔案保險箱可以被開啟(掛載)或上鎖(卸載)

要更了解這個程序，想像一個真實的銀行保險箱－它的門可以打開或上鎖。當然保險箱中的內容只有在上鎖時是安全的，但是也只有在打開時才能存取內容。

點擊將保險箱上鎖，精靈將會帶領您將特定保險箱上鎖。

步驟 1/3 —選取保險箱

您可以在此選取要上鎖的保險箱。



選取保險箱

如果您選取瀏覽檔案保險箱您必須點擊瀏覽並選取檔案保險箱。

如果您點擊選取原有的檔案保險箱您必須點擊指定的保險箱名稱。

點擊 下一步。

步驟 2/3 —總結

您可以在此回顧選取的操作。



總結

點擊 下一步。

步驟 3/3 —結果

您可以在此檢視操作結果。


BitDefender 2009
檔案保險箱 - 上鎖保險箱
步驟 1
步驟 2
步驟 3
顯示操作結果
操作
關閉保險箱
名稱
fvtest2
路徑
H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
結果
成功完成操作。
錯誤碼
資訊
保險箱已成功上鎖
進行精靈的下一個步驟。
bitdefender
完成

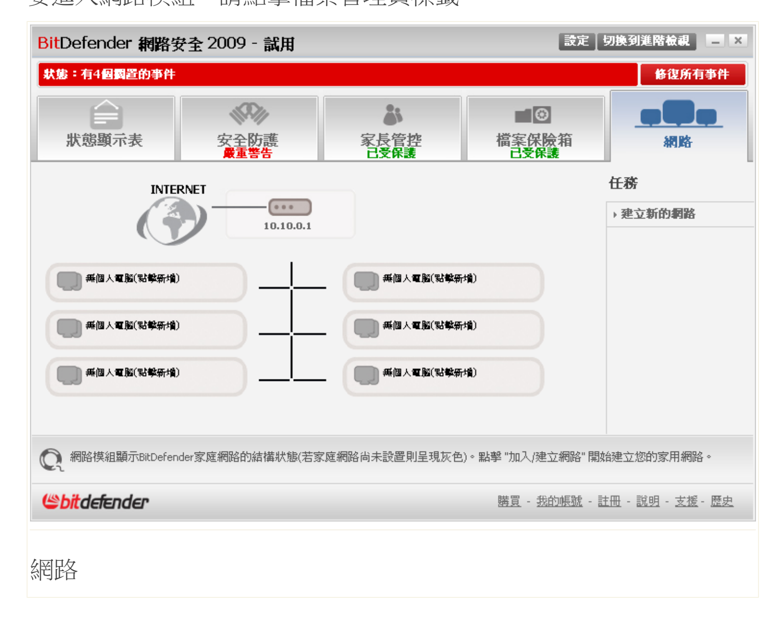
結果

點擊 完成。

10. 網路

網路模組提供您管理每一台家庭電腦中安裝的BitDefender。

要進入網路模組，請點擊檔案管理員標籤。



網路

要管理您家庭電腦安裝的BitDefender，請您依照下列步驟：

1. 在您的電腦加入BitDefender家庭網路。 加入網路，為家庭網路管理設置一個管理者密碼。
2. 使用您想管理與加入網路的電腦，並設定密碼。
3. 回到您的電腦，並新增這些您想管理的電腦。

10.1. 任務

一開始只有一個按鈕可使用。



■加入/建立網路 - 提供您設定網路密碼以進入網路。

加入網路之後，將出現其他的按鈕。

■離開網路 - 提供您離開網路。
■管理網路 - 提供您新增電腦至您的網路。
■掃描全部 - 提供您同時掃描所有管理中的電腦。
■全部更新 - 提供您同時更新所有管理中的電腦。
■全部註冊 - 提供您同時註冊所有管理中的電腦。

10.1.1. 加入BitDefender 網路

要加入BitDefender 家庭網路，請依照下列步驟：

1. 點擊加入/建立網路。 將提示您設置家庭管理密碼。



設置密碼

2. 在兩個文字框中輸入相同密碼。
3. 點擊確定。

您可以在網路地圖上看到電腦名稱。

10.1.2. 加入電腦至BitDefender 網路

加入電腦至BitDefender 網路前，您必須先在每一台電腦設置BitDefender家庭管理密碼。

要加入電腦至BitDefender 網路，請依照下列步驟：



1. 點擊管理網路。 將提示您輸入本地家庭管理密碼。

BitDefender

您必須輸入家庭管理的密碼。

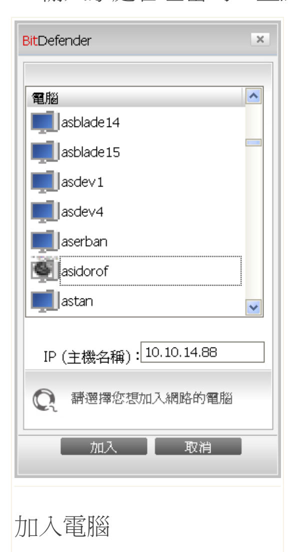
密碼: ●●●●●●●●●●●●●

不要再顯示此訊息。

確定 取消

輸入密碼

2. 輸入家庭管理密碼，並點擊確定。 一個新的視窗將會開啟。



加入電腦

您可以檢視網路中的電腦清單。 小圖示的意義如下：

顯示一台線上電腦，但未安裝BitDefender。

顯示一台線上電腦，已安裝BitDefender。

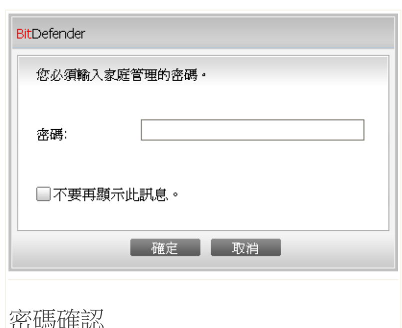
■ 顯示一台離線電腦，已安裝BitDefender。

3. 您可以選擇以下動作：

■從清單中選擇要加入的電腦名稱。

■在對應欄位輸入要加入的電腦IP位置或電腦名稱。

4. 點擊加入。 將提示您輸入電腦的家庭管理密碼。



密碼確認

5. 輸入該電腦的家庭管理密碼。

6. 點擊確定。 若密碼輸入正確，該電腦將出現在網路地圖上。



註
您最多可以加入五台電腦至網路地圖。

10.1.3. 管理BitDefender網路

只要您成功建立一個BitDefender家庭網路，您就可以管理所有電腦中的BitDefender。



網路區域

移動游標至網路地圖上的電腦，您可以查看該電腦的資訊概要(名稱、IP位置、系統安全事件數量、BitDefender註冊狀態)。

在網路地圖上的電腦名稱點擊右鍵，您可以查看所有能在遠端電腦上執行的管理任務。

■註冊這台電腦

■設置設定密碼

■執行掃描任務

■在這台電腦上修復事件

■檢視此電腦歷史

■立即於此電腦執行更新

■套用至設定檔

■在此電腦執行調整任務

■設定此電腦為此網路的更新伺服器

在執行特定電腦的任務以前，將提示您輸入本地家庭管理密碼。

BitDefender

您必須輸入家庭管理的密碼。

密碼:

不要再顯示此訊息。

確定 取消

輸入密碼

輸入家庭管理密碼，並點擊確定。



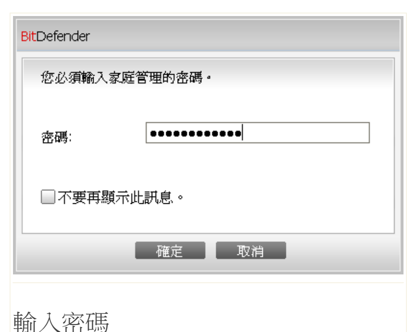
註

若您要執行多個任務，您可以選擇這段期間不要再顯示這個訊息。 這樣，這段期間將不會再提示您輸入密碼。

10.1.4. 掃描所有電腦

要掃描所有管理中的電腦，請依照下列步驟：

1. 點擊掃描全部。 將提示您輸入本地家庭管理密碼。

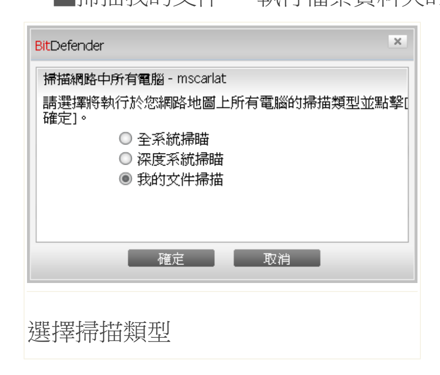


輸入密碼

2. 選擇一個掃描類型。
   ■全系統掃描 - 執行一個完整的系統掃描(除了資料封存)。



■深度掃瞄 - 執行針對您電腦系統的完整掃瞄(包含資料封存)。
■掃描我的文件 - 執行檔案資料夾的快速掃描。



選擇掃描類型

3. 點擊確定。

10.1.5. 更新所有電腦

要更新所有管理中的電腦，請依照以下步驟：

1. 點擊全部更新。 將提示您輸入本地家庭管理密碼。



輸入密碼

2. 點擊確定。

10.1.6. 註冊所有電腦

要註冊所有管理中的電腦，請依照以下步驟：

1. 點擊註冊全部。 將提示您輸入本地家庭管理密碼。



輸入密碼

2. 輸入您想註冊的序號。



全部註冊

3. 點擊確定。

11. 基本設定

在基本設定模組，您可以輕易的啟動或停用重要安全模組。

要進入基本設定模組，請從基本檢視的上方點擊設定鈕。



基本設定

可用的安全模組已分至數個類別。

種類	描述
本機安全	在這裡您可以啟動/停用即時檔案防護或自動更新。
線上安全	在這裡您可以啟動/停用即時電子郵件和網頁保護。
家長管控設定	您可以在此啟動/停用家長管控。
網路安全。	您可以在此啟動/停用防火牆
基本設定	在這裡您可以啟動/停用遊戲模式、筆電模式、密碼、掃描活動列與其他。

點擊 "+" 號方塊展開種類， "-" 號方塊關閉。

11.1. 本機安全

您可以點擊以啟動/停用安全模組。

安全模組	描述
即時病毒防護與反間諜程式檔案保護	即時檔案防護確保您存取的所有檔案、應用程式執行的檔案都經過掃描。
自動更新	自動更新確保BitDefender產品及特徵碼檔案會定期下載並安裝更新。
自動系統弱點檢查	自動系統弱點檢查確保您電腦中的重要軟體的更新。

11.2. 線上安全

您可以點擊以啟動/停用安全模組。

安全模組	描述
即時病毒防護，反垃圾郵件&反網路釣魚郵件防護	即時郵件防護確保您的電子郵件已受到垃圾郵件及網路釣魚企圖的掃描。
即時病毒防護&反間諜程式網站防護	反間諜程式網站防護確保您透過HTTP 所下載的所有檔案都已經過病毒及間諜程式掃描。
即時反網路釣魚保護	即時反網路釣魚保護確保您透過HTTP下載的所有檔案都被掃描。
身分管控	身分管控掃描所有網頁和電子郵件傳輸的特定字串，幫助您維護隱私資料的安全。
即時通訊加密	如果您的即時通訊連絡人已安裝了BitDefender，所有透過Yahoo即時通與Windows Live Messenger(MSN)的即時交談訊息都將被加密。

11.3. 家長管控設定

您可以點擊以啟動/停用家長管控模組。

家長管控能夠阻擋存取不適當的網頁或在特定時間存取網際網路，並掃描電子郵件、即時通訊及網路傳輸中的特定字詞。

11.4. 網路設定

您可以點擊以啟動/停用防火牆模組。

防火牆確保您免於駭客或惡意程式的攻擊。

11.5. 檔案保險箱設定

您可以點擊以啟動/停用檔案保險箱。

檔案保險箱透過加密檔案來保護您的文件與資料。

11.6. 一般設定

您可以點擊以啟動/停用相關的安全項目。

項目	描述
遊戲模式	遊戲模式能夠暫時地變更防護設定，在您進行遊戲時將系統運行的影響減至最低。
筆電模式	筆電模式能暫時變更防護設定，降低對筆電電池壽命的影響。
設定密碼	確保BitDefender設定將經過密碼保護。
家長管控密碼	啟動這個選項可以保護家長管控模組的設定。確保家長管控的設定只能經由知道密碼的使用者變更。
BitDefender新聞	啟動這個選項，您將收到重要的BitDefender公司訊息、產品更新訊息或新的安全威脅訊息。
產品提示警示	啟動這個選項，您將收到資訊警示。
掃描活動列	小且清晰的掃瞄活動列能顯示BitDefender 掃描活動的進程，綠色流線顯示本機系統掃描、紅色流線則顯示網路連線的掃描。
在系統啟動後載入BitDefender	啟動這個選項，BitDefender將在系統啟動時載入。這個選項不會影響防護層級。
傳送病毒報告	啟動這個選項，將傳送病毒掃描報告至BitDefender實驗室進行分析。這個報告將不會含有隱私資料，例如您的名字或IP位置，也不會被用來進行商業活動。

項目	描述
病毒疫情偵測	啟動這個選項，潛在病毒疫情報告將傳送至BitDefender實驗室進行分析。這個報告將不會含有隱私資料，例如您的名字或IP位置，也不會被用來進行商業活動。



12. 狀態列

您會注意到，BitDefender 網路安全2009的視窗上方有一個狀態列顯示尚未解決的事件數量。點擊修復所有事件鈕以移除所有可能威脅您電腦安全的事件。將會出現一個安全防護狀態視窗。

安全防護狀態顯示一有系統組織和在您的電腦上的安全弱點的容易辨識目錄。 每當一個問題會影響您電腦的安全， BitDefender 網路安全 2009 將讓您知道。



狀態列

12.1. 本機安全

在任何問題出現可能影響您的電腦安全時，及時提醒您是非常重要的。藉由監控每個安全防護模組，BitDefender 網路安全2009不只在您的設定可能影響您的電腦安全時提醒您，如果您遺忘了重要的任務也會同時受到提醒。

關於本機安全的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
即時檔案防護已啟動	保證系統中所有您存取的檔案、或者應用程式執行的程式都已被掃描。
您今天已經掃瞄您電腦中的惡意程式	強烈建議您立即執行手動掃描，確認您電腦中的檔案是否不受惡意程式威脅。
自動更新已啟動	請維持自動更新啟動，確保惡意程式特徵碼是最新的狀態。
立即更新	產品及惡意程式特徵碼更新正在進行。
防火牆已啟動	保護您的電腦遠離惡意程式及駭客。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

12.2. 線上安全

關於線上安全的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
反垃圾郵件已啟動	確保您的電子郵件經過掃描沒有惡意程式，並過濾垃圾郵件。
身分管控已啟動	透過掃描網路及郵件傳輸中的特別字串，幫助您維護私密檔案的安全。建議您啟動身分管控以保護您的私密檔案(例如：電子郵件地址、使用者名稱、密碼、信用卡號碼)安全不被偷竊。
Firefox反網路釣魚保護已啟動	BitDefender能夠防護您的電腦免於網路釣魚的威脅。
Internet Explorer 反網路釣魚保護已啟動	BitDefender能夠防護您的電腦免於網路釣魚的威脅。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

12.3. 檔案保險箱

可能影響您的資料隱私權的事件會描述的非常清楚。如果有任何事物可能影響您的資料隱私權，你將會看到一個紅色的狀態按鈕稱為修復。 或者顯示綠色的OK狀態鈕。

事件	描述
檔案保險箱已啟動	檔案保險箱透過加密檔案來保護您的文件與資料。

當狀態按鈕是綠色時，您的資料安全危險已降到最低。要把按鈕變成綠色，請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。

12.4. 系統弱點掃瞄

關於系統弱點的事件敘述十分清晰，若有安全威脅的事件，您將看到修復的紅色狀態鈕。 或者顯示綠色的OK狀態鈕。

事件	描述
系統弱點檢查已啟動	監控Microsoft Windows更新、Microsoft Office更新及Windows帳戶密碼，以確保您的作業系統經過更新、密碼安全。
重要的Microsoft更新	安裝可用的重要Microsoft更新。
其他Microsoft更新	安裝可用的次要Microsoft更新。
Windows自動更新已啟動	若有新的Windows安全性更新，立即安裝。

事件	描述
管理者（安全的密碼）	顯示特定使用者密碼的強度。

狀態鈕是綠色，表示您的系統危險性小。讓狀態鈕變綠請依照下列步驟：

1. 點擊修復鈕以逐一修復安全弱點。
2. 如果有一個問題不能被修復，請跟隨精靈的指示來修復。

若您想要從監控排除一個事件，請取消選取是，監控此元件。



13. 註冊

BitDefender網路安全 2009 有30天的試用期限 如果您想要註冊BitDefender網路安全 2009、變更授權序號或建立BitDefender帳號，點擊位於 BitDefender 安全防護中心視窗的上方的 註冊。 註冊精靈將會出現。

13.1. 步驟 1/1 - 註冊 BitDefneder 網路安全 2009



註冊

您可以檢視BitDefender 註冊狀態，現在使用的授權序號，以及授權序號將在幾天內到期。

註冊 BitDefneder 網路安全 2009：



1. 選取 我想要以新的序號註冊產品。
2. 在編輯欄位中輸入授權序號。



註
您可以在這些地方找到授權序號：
■光碟標籤。
■產品註冊卡。
■線上購買的電子郵件。

如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

點擊 完成。



14. 歷史紀錄

在BitDefender安全防護中心視窗下方的 歷史紀錄鈕將可以開啟另一個視窗BitDefender歷史紀錄& 事件。這個視窗提供您概括性的檢視與安全性相關的事件。 例如您可以輕易地檢查最近是否有成功的更新，有沒有惡意程式在您的電腦裡頭被發現等等。



事件

為了協助您過濾BitDefender歷史紀錄&事件，視窗左側將提供以下目錄：

■病毒防護
■防火牆
■反垃圾郵件
■隱私權管控
■家長管控
■更新
■網路。

■檔案保險箱

每一個目錄都有一個可用的事件清單，每個清單包含下列資訊：簡短的敘述、BitDefender所執行的動作、發生的時間日期。如果您想了解更多只需要在事件上點擊兩下即可。

點擊 清除紀錄 以清除舊的紀錄。點擊 重新整理 以顯示最新的日誌。

進階管理

15. 一般

一般模組提供有關BitDefender 的動作以及系統的相關資訊。 您也可以在此變更BitDefender 的整體行動。

15.1. 狀態顯示表

要檢視產品動作的統計數據以及您的註冊狀態，請在進階檢視選擇一般>狀態顯示表



狀態顯示表

狀態顯示表包含包含了幾個頁面。

■統計數據－顯示重要的BitDefender動作相關數據。

■總覽 — 檢視更新狀態、您的帳號狀態以及註冊相關資訊。

- 檔案區－表示BitDefender所掃描到的惡意程式數量變化，長度代表時間區段內發現的密度。
- 網路區－表示防火牆掃描過的網路傳輸，長度代表時間區段內傳輸的密度。

15.1.1. 統計數據

如果您想持續追蹤BitDefender的動作，統計數據頁面會是個好開始。 您可以檢視下列項目：

項目	描述
已掃描的檔案。	表示上一次掃描所檢查的檔案數量。
消毒的檔案。	表示上一次掃描成功消毒的檔案數量。
已偵測的病毒。	表示上一次掃描所檢查出的病毒數量。
已阻擋的連接埠掃描	表示已被防火牆阻擋的連接埠掃描數量。 連接埠掃描時常被駭客來尋找您開啟的連接埠。 保持防火牆以及匿蹤模式啟動以對抗連接埠掃描。

15.1.2. 概觀檢視

這裡您可以查看關於更新、帳戶、註冊狀態及授權序號資訊的統計資料概況。

項目	描述
上次更新	顯示您上次更新產品的日期。請定期更新以完整保護您的系統。
我的帳號	顯示用來存取線上帳戶的電子郵件地址，您可以使用它存取您的線上帳戶以重新取得您遺失的BitDefender授權序號、得到BitDefender支援及其他服務。
註冊	顯示您的授權序號及狀態。若您的序號已過期，請續購或升級產品以保護您的系統安全。
到期	顯示授權序號到期的天數。

15.2. 設定

要設置並管理一般設定，請在進階檢視選擇一般>設定。



一般設定

在這裡可以設定所有 BitDefender 喜好。預設上，BitDefender 會在視窗啟動時被載入，並執行最小化在系統工具列上。

15.2.1. 一般設定

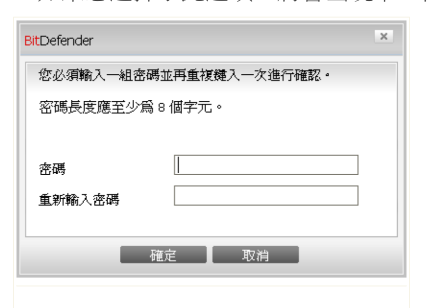
■啟動密碼保護 — 此選項為了保護 BitDefender 管理主控台的設定。



註

如果您不是此電腦唯一擁有管理權限的人，建議您設定密碼保護您的 BitDefender 設定。

如果您選擇了此選項，將會出現下一個視窗：



輸入密碼

在密碼欄位上，輸入密碼，在重新輸入密碼欄位上，重新輸入密碼，並點擊確定。

一旦您設了密碼，每次您要變更BitDefender設定時，您都會被要求輸入密碼。 其他的系統管理者(如果有)若要變更設定也是需要此密碼。

如果您只想在設置家長管控時被提示輸入密碼，請選取只要求/套用密碼到家長管控。　　另一方面，如果密碼只為家長監控設置但您沒選取這個選項，當設置所有BitDefender選項時，都會要求密碼。



重要

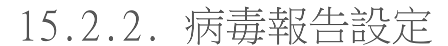
如果忘記密碼，您必須修復此軟體才可進行 BitDefender 的設定。

- 當家長監控啟動時，將要求密碼 - 如果這個選項已啟動，並且沒有設定密碼，當啟動家長監控時，您將被提示設定密碼。 設定一個密碼，您可以阻止其他使用者變更您對特定使用者設置的家長管控設定。
- 顯示 BitDefender 消息 (安全通知) — 由 BitDefender 伺服器寄送關於病毒疫情擴散的即時安全通知。
- 顯示彈出式視窗 (螢幕上的提示) — 在彈出式視窗顯示軟體狀態。 您可以設置BItDefender只在進階或是基本檢視顯示彈出式提示。
- 在 Windows 啟動後載入 BitDefender — 在系統啟動後，自動地開啟 BitDefender。 我們建議您保留此選項的選擇。
- 啟動掃描活動列 (螢幕上顯示掃描活動的狀態 — 啟動/關閉 掃描活動列。 您可以取消這個核取方塊如果您不想看見掃描活動列。



註

此選項只能被目前的Windows使用者調整。



15.2.2. 病毒報告設定

- 寄送病毒報告 — 當您的電腦發現病毒時，寄發病毒報告到 BitDefender 實驗室。它將協助我們保持病毒疫情擴散的追蹤。

  這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。這個資訊只包含病毒名稱，並且僅僅用來建立統計報告。

- 啟動 BitDefender 疫情擴散偵測 — 將潛在病毒疫情擴散報告寄送到 BitDefender 實驗室。

  這份報告將不包含機密資料，如：您的姓名、IP 位址或其他，而且此份資料不會被使用在商業目的上。這個資訊只包含潛在病毒並且僅僅用來偵測新的病毒。

15.3. 系統資訊

BitDefender 使您從單一個地方便能夠檢視開機時所有的系統設定以及登錄執行的應用程式。如此，您可以監控所有系統的活動並能夠辨識感染的發生。

要獲得系統資訊，請在進階檢視選擇一般>系統資訊。





系統資訊

這個清單包含所有被載入的項目，當系統啟動時，這些項目會被不同應用程式所載入。可用三個按鈕：

■還原－變更目前的檔案關聯至預設值。 只在檔案關聯設定可用。

■到 — 開啟您所選擇項目的視窗（如：登錄）



註
隨著所選的項目不同， 到按鈕不一定會出現。

■重新整理 — 重新整理 系統資訊 頁面。

16. 病毒防護

BitDefender保護您的電腦對抗所有惡意程式的威脅 (病毒、間諜程式、木馬程式及其他)。 BitDefender 的安全防護可分為二類：

■即時防護－保護您的系統不受新進入的惡意程式威脅。 舉例來說，當您打開它的時候， BitDefender 將會掃描您正在開啟的 Word 檔案，以及您接收中的電子郵件。



註
即時防護同時也包括了存取掃描－當檔案被使用者存取時，就會受到掃描。

■手動掃描－允許掃描並移除已在您的系統的惡意程式。 這是由使用者啟動的典型掃描－您手動選擇要掃描的磁碟、資料夾或檔案，而BitDefender 進行掃描。 您可以建立個人化的例行掃描時程。

16.1. 即時防護

BitDefender提供持續性的即時防護，透過掃描存取的檔案、電子郵件訊息和即時通訊應用程式(ICQ, NetMeeting, Yahoo即時通, MSN Messenger)，以對抗多種類的惡意程式威脅。 BitDefender 反網路釣魚能夠在您瀏覽可能帶有竊取個人訊息的網頁時，警告您潛在的網路釣魚網站。

要設置即時防護及BitDefender反網路釣魚，請在進階檢視選擇病毒防護>防禦。



即時防護

您可以檢視即時防護是已啟動或停用。 如果您想變更即時防護狀態，選取或清除對應的核取方塊。



重要

為了防止病毒感染您的系統，請保持即時防護 啟動。

要開始快速系統掃瞄，點擊立即掃瞄。

16.1.1. 設置防護層級

您可以選擇最適合您安全需求的防護層級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

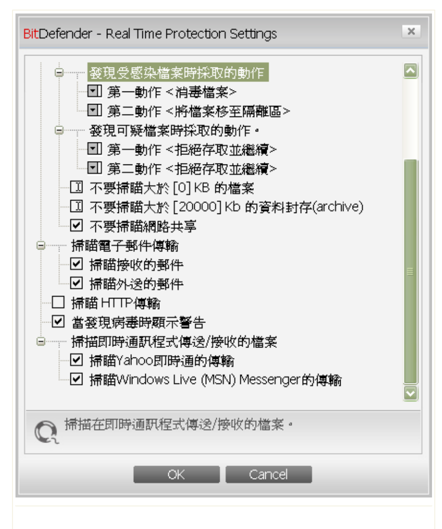
防護層級	描述
寬鬆	僅含概基本的安全需求，資源耗用層級非常低。 只有應用程式和接收的電子郵件會被掃描。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。
預設	提供標準的安全防護。資源耗用層級較低。 所有檔案、接收及傳送的電子郵件都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。
嚴謹	提供較高的安全防護。耗用資源層級中等。 所有檔案、接收及傳送的電子郵件及網站的傳輸都會被掃描是否有病毒或間諜程式。除了傳統的特徵掃描外，也使用啟發式的分析。受感染的檔案將採取以下的動作：清除檔案/禁止存取。

如果您想要回復到預設層級，點擊 預設層級。

16.1.2. 自訂防護層級

進階的使用者可以使用 BitDefender 所提供的掃描設定。掃描器中可以設定指定特定的副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

您可以自訂 即時防護，點擊 自訂層級。將會出現下一個視窗：



防禦設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。



註

您會注意到雖然一些掃描選項前面出現 "+"，但卻無法被展開。這是因為這些選項尚未被選取。您會注意到，如果您選擇了這些選項，則其細項即可被展開。

■掃描存取的檔案及點對點的傳輸選項 — 掃描被存取的檔案及透過即時傳訊軟體溝通的應用程式 (ICQ、NetMeeting、Yahoo 即時通、MSN Messenger)。選擇您所要掃描的檔案型態。

選項		描述
掃描存取的檔案	掃描所有檔案	所有存取的檔案都將被掃描，不管其型態為何。
	只掃描應用程式檔案	只有應用程式檔案將被掃描。代表只有以下副檔名的檔案才會被掃描：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd;

選項		描述
		.sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。
	掃描危險程式	掃描危險程式。 被偵測掃描的危險程式將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。 選擇 掃描中跳過撥號程式及應用程式，以在進行掃描時排除這類型的檔案。
掃描開機區域		掃描系統開機磁區。
掃描內部資料封存		被存取的資料封存將被掃描。當這個選項啟動時，電腦將會變慢。
掃描壓縮檔案		所有壓縮檔案將會被掃描。
第一動作		從下拉式選單選擇當遇到受感染及可疑檔案時，第一動作所要採取的動作。
	禁止存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。
	清理檔案	消毒被感染的檔案。
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。
	移動檔案到隔離區	移動受感染的檔案到隔離區。
第二個動作		從下拉式選單選擇當遇到受感染的檔案時，所要採取的第二動作。(當第一動作失敗時)
	禁止存取並繼續	當偵測到受感染的檔案，對它的存取動作也將被禁止。
	刪除檔案	立刻刪除受感染的檔案，不經任何警告。

選項	描述
移動檔案到隔離區	移動受感染的檔案到隔離區。
不要掃描大於 [x] Kb 的檔案	輸入要被掃描的最大檔案大小。如果大小為 0Kb, 代表所有檔案將被掃描，而不管這些檔案的大小。
不要掃描大於[20000] Kb 的檔案	輸入要被掃描的最大檔案大小(KB)。 如果您要掃描所有檔案，而不管它們的大小，輸入0。
不要掃描網路共用檔案	如果啟動此選項，BitDefender 將不掃描網路共用檔案，提供您更快的網路存取速度。 如果您的網路作業環境已經有病毒防護措施，我們才建議您啟動此選項。

■掃描電子郵件傳輸 — 掃描電子郵件的傳輸。

以下的選項是可用的：

選項	描述
掃描接收的電子郵件	掃描所有接收的電子郵件訊息。
掃描傳送的電子郵件	掃描所有傳送的電子郵件訊息。

■掃描 Http 傳輸 — 掃描 Http 傳輸。

■當發現病毒時提出警告 — 在檔案或電子郵件中發現病毒時，開啟一個警示視窗。

一個受感染的警告視窗將包含病毒名稱、發現的路徑、BitDefender 所採取的行動及一個連結到 BitDefender 的網站，在那裡您可以得到更多關於此病毒的資訊。在一個受感染的電子郵件警示視窗裡也包含了寄件者及收件者的資訊。

當偵測到一個可疑的檔案時，您可以從警告視窗裡開啟一個精靈，它將協助您寄送檔案到 BitDefender 實驗室進行分析。您可以輸入您的電子郵件位址以得到這個報告的相關資訊。

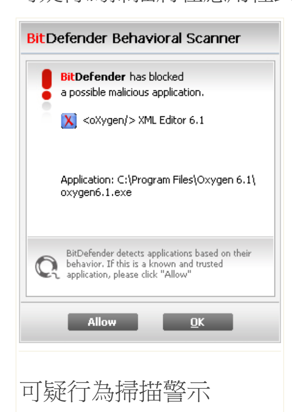
■掃描經由即時通訊接收或傳送的檔案. 要掃描經由Yahoo 即時通或Windows Live Messenger接收或傳送的檔案，請選取對應的核取方塊。

點擊 確定以儲存變更並關閉視窗。

16.1.3. 設置可疑行為掃描

可疑行為掃描提供您針對擁有未發佈的特徵的惡意程式的防護。 它將持續監控並分析在您電腦上運行的應用程式行為，當應用程式出現可疑行為時提出警告。

可疑行為掃描將在應用程式嘗試執行可能的惡意行動時提出警告，並提示您作出動作。

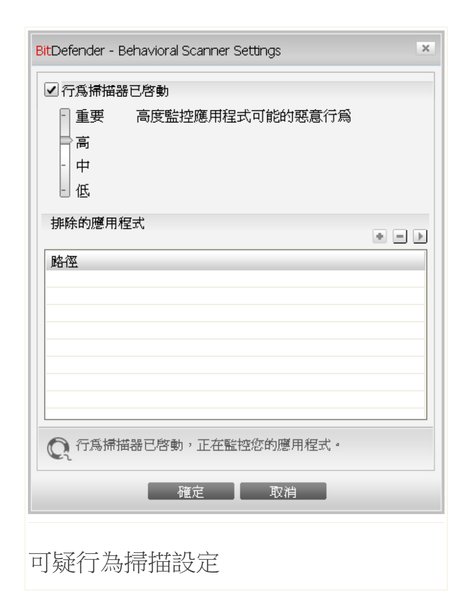


可疑行為掃描警示

如果您知道並信任被偵測到的應用程式，點擊允許。 可疑行為掃描將不會再掃描嘗試執行可能惡意行動的應用程式

如果您想要立刻關閉這個應用程式，點擊確定。

要設置可疑行為掃描，點擊 掃描設定。



可疑行為掃描設定

如果您想要停用可疑行為掃描，清除啟動可疑行為掃描核取方塊。



重要
保持可疑行為掃描啟動以防護未知的病毒。

設置防護層級

可疑行為掃描防護層級會自動隨著即時防護層級變更。 如果不滿意預設的設定，您可以手動設置防護層級。



註
請注意如果您變更了即時防護層級，可疑行為掃描防護層級會自動隨著變更。

拖曳滑桿以設定您認為適當的防護層級。

防護層級	描述
重要	應用程式將嚴格的被監控是否有可能的惡意行為。

防護層級	描述
高	應用程式將嚴厲的被監控是否有可能的惡意行為。
中	應用程式將中等的被監控是否有可能的惡意行為。
低	應用程式將被監控是否有可能的惡意行為。

管理例外應用程式

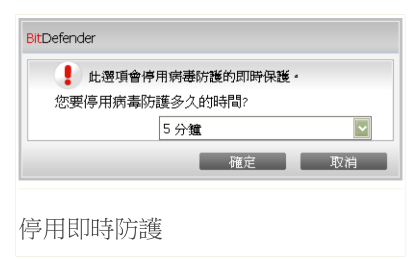
您可以設置可疑行為掃描不檢查特定的應用程式。 目前不被可疑行為掃描檢查的應用程式被列表在例外應用程式。

要管理例外應用程式，您可以使用清單下方的按鈕。

- Add - exclude a new application from scanning.
- Remove - remove an application from the list.
- Edit - edit an application path.

16.1.4. 停用即時防護

如果您想要停用即時防護，將會出現一個警告視窗。



停用即時防護

您可以從視窗選擇您要停用即時防護的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。



警告

這是個重大安全事件。我們建議您盡量縮短停用即時防護的時間。如果您停用即時防護，您的電腦將暴露於各種惡意程式威脅之中。

16.1.5. 設置反網路釣魚防護

BitDefender 為以下程式提供即時反網路釣魚防護：

- Internet Explorer
- Mozilla Firefox
- Yahoo 即時通
- Windows Live (MSN) Messenger

您可以針對特定或所有的應用程式停用反網路釣魚防護。

您可以點擊白名單以設置並管理不被BitDefender反網路釣魚引擎掃描的網站清單。



反網路釣魚白名單

您可以檢視所有不會被BitDefender反網路釣魚引擎掃描的網站。

要將網站加入白名單，在新的位址欄位輸入網站的網址並點擊加入。 白名單應該只包含您完全信任的網站。 舉例來說，加入您最近使用過的線上商店網站。



註

您可以利用BitDefender設立在瀏覽器的反網路釣魚工具列可以容易地管理防護工具，以及建立白名單。

如果您想從白名單中移除網站，點擊對應的移除鈕。

點擊 關閉以儲存變更並關閉視窗。

16.2. 手動掃描

BitDefender 的主要目的是維護您的電腦免受到病毒的威脅。保持新的病毒遠離您的電腦是最首要的目標，透過掃描電子郵件、新下載的檔案或複製到您系統的檔案。

在您安裝 BitDefender 前，可能已經有病毒存在於您的系統中。這是為什麼在您完成安裝 BitDefender 後，要求掃描您的系統，以找出存在的病毒。經常掃描您的電腦是個很好的建議。

在進階檢視點擊病毒防護>掃描，可以設置以及啟動手動掃描。



掃描任務

手動掃描是以掃描任務為基礎。掃描任務決定要被掃描的物件以及掃選項。 您可以用預設的掃描任務或是您(使用者)自訂的掃描任務來掃描電腦。您也可以規劃它們用基本的方式進行或是當您的電腦閒置時，以避免影響您的作業。

16.2.1. 掃描任務

在系統預設情況下BitDefender以幾項任務，建立包含一般的安全問題。 您也能建立您自訂的掃瞄任務。

每項任務有屬性允許您配置任務和看掃描結果的視窗。 對於更多信息，查看"設定掃描任務" (p. 135).

掃描任務有三個類別：

■系統任務 — 包含預設的系統掃描。下方是可用的掃描任務：

預設的任務	描述
深度系統掃描	掃描整個系統。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
全系統掃瞄	掃描整個系統，資料封存除外。 在預設的設置中，它能夠掃描您電腦中所有種類的惡意威脅。
快速的系統掃描	掃描Windows ， Program Files 以及 All Users 資料夾。 在預設的設定中，可以掃描除後門程式外所有的惡意程式，但是不會掃描記憶體、登錄碼、cookies.
自動登入掃描	掃描使用者登入Windows就執行的項目。 自動登入掃描預設為停用的。 若您要使用此任務，按右鍵選擇排程，將任務設為於系統啟動時執行。 您可指定在系統啟動多久(分鐘)之後開始執行。



註
由於深度掃瞄與全系統掃瞄 是針對系統整體的分析任務，所以會需要較長的時間，我們建議您可以以低優先率執行此任務，或在您的系統閒置時執行。

■用戶的任務 — 包含用戶定義的任務。

有一個叫做 我的文件的掃描任務。 使利用這個掃描任務執行掃描重要的使用者資料夾，如：我的文件 、桌面 以及 啟動。

- 其他的任務 — 包含其他掃描任務的清單。這些掃描任務參考到其他替代的掃描型態，而且它無法在這個視窗中執行。您只可以修改它們的設定及檢視掃描報告。

每個掃描任務的右邊有三個可按的按鈕：

- 排程任務 — 選擇將以排程來執行的任務。 從 屬性視窗裡，按下 排程器 頁面，您可以修改這個設定。
- 刪除 — 刪除所選擇的掃描任務。

> 註
> 系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

- 立即掃描 — 執行所選的掃描任務，進行一個 立刻掃描。

在每個任務的左方您可看見屬性 — 允許您去設定任務以及檢視掃描日誌。

16.2.2. 使用捷徑選單

每個掃描任務都有一個捷徑選單可使用。在選擇的掃描任務按下滑鼠右鍵去開啟它：



捷徑選單

在捷徑選單上有以下可用的命令：

- 立即掃描 — 立刻掃描所選的掃描任務。

-

■路徑 — 開啟 屬性 視窗，路徑 標籤頁，您可以更改所選掃描任務的掃描目標。



註
在系統掃描任務頁面，這選項將會顯示掃描路徑被替代，而只能看見掃描目標。

■排程 — 選擇將要排程執行的任務。 從 屬性視窗裡，點擊 排程器 標籤，您可以在此進行任務排程。

■日誌 — 開啟屬性 視窗，日誌 標籤頁，在掃描任務執行後，您可以檢視產生的報告。

■複製 — 複製所選擇的掃描任務。 當建立新的掃描任務時，您可以方便地修改已複製的掃描任務的設定。

■刪除 — 刪除所選擇的掃描任務；



註
系統掃描任務無法使用此功能。您不能刪除一個系統掃描任務。

■開啟 — 開啟屬性視窗，檢視 標籤頁，您可以更改所選掃描任務的設定。



註
尤於特性不同，在 其他任務 的類別裡，只有 開啟 及 日誌 二種選項可使用。

16.2.3. 建立掃描任務

您可以選擇以下其中之一種方法建立掃描任務：

■複製 一個存在的掃描任務，您可以在 屬性 視窗中更改它的名稱或做必要的修改設定；
■按下 新的任務 ，建立一個新的掃描任務並且設定它。

16.2.4. 設定掃描任務

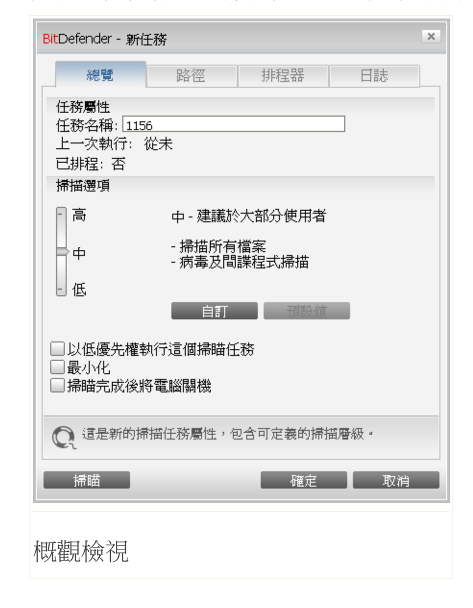
每個掃描任務都有它的 屬性 視窗，您可以設定掃描的選項、掃描的目標、指定排程或檢視報告。從這個視窗裡的任務名稱按二下。下面的視窗將會出現： 按下右邊的開啟鈕，開啟視窗(或是在任務上點擊滑鼠右鍵，選擇開啟)。



註
更多關於 日誌 頁面的資訊，請參考 "檢視掃描日誌"（p. 152）。

調整掃描設定

要調整任何特定的掃描任務，請按下滑鼠右鍵，並選擇屬性。 以下視窗將會顯示：



概觀檢視

在這裡，您可以檢視掃描任務的資訊（名稱、上次執行的時間及排程狀態）及設定掃描的設定。

選擇掃瞄層級

首先，您必須選擇掃瞄的層級。拖曳滑桿到合適的掃瞄層級。

一共有三個掃瞄層級：

防護層級	描述
低	提供適當的偵測效率。耗用系統資源資源低。

防護層級	描述
	應用程式只被掃描是否有病毒。除了基本的特徵掃描，也使用了啟發式的分析。
中	提供良好的偵測效率。耗用系統資源層級屬中等。 所有檔案都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。
高	提供高水準的偵測效率。耗用系統資源層級較多。 所有檔案及封存檔都被掃描是否有病毒及間諜程式。除了基本的特徵掃描，也使用了啟發式的分析。

在掃描程序中可用到的一系列設定選項：

- 以低優先權執行任務. 降低掃描程序的優先權。您可以讓其他程式執行的更快，但這個掃描程序將會花更長的時間去完成。
- 將視窗最小化到系統工具列. 將掃描視窗最小化到 系統工具列。可以按二下 BitDefender 圖示去開啟它。
- 當掃描完成時若沒有發現病毒，將這台電腦關機

按下 確定儲存變更並關閉視窗。要執行任務，請點擊掃描 。

自訂掃瞄層級

進階的使用者可以使用 BitDefender 所提供的掃描設定。掃描器中可以設定指定特定的副檔名、目錄或您所知道無害的檔案。這將會減少掃描時間並加快您系統掃描的反應時間。

按下 自訂，將會出現一個新視窗，您可以設定自己的掃描選項：

掃描設定

掃描的選項以可擴展的選單方式呈現，非常相似於 Windows 檔案總管。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。

掃描選項被分為三種類型：

■掃瞄層級.　從掃瞄層級選單選擇適合的選項，指定您要BitDefender掃瞄的惡意程式類型。

選項	描述
掃描病毒	掃描已知病毒威脅。 BitDefender也能夠偵測到不完整的病原體，因此能夠移除您系統內的可能威脅。
掃描廣告程式	掃描廣告程式。被偵測到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含廣告元件的軟體將無法運作。
掃描間諜程式	掃描已知的間諜程式。被偵測到的檔案將被當成受感染的檔案。

選項	描述
掃描應用程式	掃描可能會被利用為間諜工具的正當程式。
掃描撥號程式	掃描高收費陷阱的撥號程式。這些被掃描到的檔案將被當成受感染的檔案。如果這個選項啟動時，包含這類型撥號程式的軟體將無法運作。
掃描後門程式	掃描隱藏的物件，一般稱後門程式。

■病毒掃描選項. 指定要被掃描的物件類型 (資料封存、檔案、電子郵件，等) 以及其他選項。這個設定可以從 病毒掃描選項 中去進行設定。

選項		描述
掃描檔案	掃描所有檔案	所有檔案都將被掃描，不管其型態為何。
	只掃描應用程式檔案	只有程式檔案才會被掃描。這代表只有以下的副檔名將被掃描：exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml 及 nws。
	掃描使用者定義的副檔名	只有被使用者指定的副檔名將會被掃描。這些副檔名必須以"；" 做區隔。
開啟被壓縮的程式		掃描壓縮的檔案。
開啟資料封存		掃描內部資料封存。 掃描被封存的檔案會需要更多時間並需要較多的系統資源。 您可以點擊封存檔大小限制的欄位，輸入要掃描的封存檔大小的最大值 (KB)。
開啟電子郵件資料封存		掃描電子郵件資料封存。
掃描開機磁區		掃描系統開機磁區。

選項	描述
掃描記憶體	掃描記憶體是否有病毒或其他的惡意程式。
掃描登錄	掃描登錄項目。
掃描 Cookies	掃描 cookie。

■動作選項. 請針對受感染或可疑的檔案應執行的指定動作。為了檢視遭遇到這些檔案時所有可能的動作，請開啟 動作選項 類別。



註
要設定新的動作，點擊目前的動作欄可從選單中選取適合的選項。

- 選擇當偵測到受感染的檔案時執行的動作： 以下的選項是可用的：

動作	描述
無（只記錄物件）	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
消毒檔案	從受感染的檔案中移除惡意程式碼。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	移動受感染的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

- 偵測到可疑檔案時所採取的行動。 以下的選項是可用的：

動作	描述
無（只記錄物件）	對於可疑檔案不會採取行動。這些檔案將出現於報告檔案。
刪除檔案	立刻刪除受感染的檔案，不需任何警告。
移動檔案到隔離區	移動可疑的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。



註
假如有檔案被探索式分析偵測為可疑的，我們建議您將這些檔案送交至BitDefender Lab。

- 選擇當偵測到隱藏的物件(後門程式)執行的動作。 以下的選項是可用的：

動作	描述
無 (只記錄物件)	在偵測到受感染的檔案時將不會有任何行動。這些檔案將會出現在報告裡。
移動檔案到隔離區	移動受隱藏的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。
顯示隱藏的檔案	顯示所有隱藏的檔案。

- 被封存的檔案動作選項. 掃描並處理資料封存內部的檔案。 受密碼保護的檔案無法被掃描。 依據封存的種類，BitDefender可能會無法消毒、隔離、刪除受感染的被封存檔案。 從封存的檔案動作選項選單選擇適合的選項。

  ○選擇當偵測到受感染的檔案時執行的動作： 以下的選項是可用的：

動作	描述
沒有採取動作	掃描記錄只保存記錄被感染封存檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
消毒檔案	從受感染的檔案中移除惡意程式碼。 由時候消毒的動作會失敗，像是受感染的檔案在郵件封存內部的時候。
刪除檔案	立刻刪除受感染的檔案，不經任何警告。
移動檔案到隔離區	隔離區資料夾 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

  ○偵測到可疑檔案時所採取的行動。 以下的選項是可用的：

動作	描述
沒有採取動作	掃描記錄只保存記錄可疑的封存檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。

動作	描述
刪除檔案	立刻刪除受感染的檔案，不需任何警告。
移動檔案到隔離區	移動可疑的檔案到隔離區。 隔離的檔案無法被執行或開啟，如此可避免被感染的風險。

○選擇當偵測到受密碼保護的檔案時執行的動作。 以下的選項是可用的：

動作	描述
記錄為未掃描的	掃描記錄只保存記錄受密碼保護的檔案。 掃描完成後，您可以開啟掃描記錄檢視掃描結果。
詢問密碼	當偵測到受密碼保護的檔案時，詢問使用對應的密碼以掃描該檔案。



註
如果您選擇忽略被偵測的檔案或是選擇的動作失敗了，您將必須在掃描精靈選擇一個行動。

如果您按下 預設層級 您將載入預設的設定值。 點擊 確定以儲存變更並關閉視窗。

設定掃描目標

要設定特定使用者掃描任務的掃描目標，請按下滑鼠右鍵，並選擇路徑。 以下視窗將會顯示：



掃描目標

您可以看見本機、網路、可拆除式磁碟中的檔案。所有被選擇的物件都會被掃描。這個頁面包含了以下的按鈕：

■加入項目 — 開啟一個瀏覽的視窗，您可以選擇所要掃描的檔案。



註
您可以將檔案拖曳增加至檔案/目錄到清單中。

■">移除項目 — 從掃描清單中移除先前所選擇的檔案或目錄。



註
只有後來被加入檔案 / 資料夾才能被刪除。

除了上面解釋過的按鈕，也有一些選項允許您快速選擇掃描位置。

■本機磁碟 — 掃描本機磁碟。
■網路磁碟 — 掃描所有網路磁碟。

■可拆除式磁碟 — 掃描可拆除式的磁碟 (光碟、軟碟)。
■所有項目 — 掃描所有磁碟，不管是本機、網路或者可拆除式的磁碟。



註
如果您想要掃描整個電腦是否有病毒，請選擇核取方塊對應的 所有項目。

按下 確定儲存變更並關閉視窗。要執行任務，請點擊掃描 。

檢視系統任務的掃描目標

您無法變更在系統任務目錄下的掃描目標 您只可以看見掃描的目標。

若要檢視特定任務的掃描目標，按下滑鼠右鍵，並選擇顯示任務路徑。 以全系統掃描為例，以下的視窗將會出現：



全系統掃描的掃描目標

全系統掃描 與 深度系統掃描 將會掃描所有的本機磁碟，而 快速系統掃描只會掃描 Windows 與 Program Files 的檔案與資料夾。

點擊 確定 關閉視窗。 要執行本任務，按下 掃描。

排程掃描任務

在複雜的掃描任務中，掃描程序將花費一些時間，如果您可以關閉其他應用程式，那掃描工作將會進行得更順利。這也就是為什麼當您沒有使用電腦或者電腦閒置時，是您進行排程掃描的最佳時機。

要看見特定的任務排程或要調整它，在任務按右鍵並選擇 排程。 以下視窗將會顯示：



排程器

您能見到排程任務，如果有的話。

當排程一個掃描任務時，您必須選擇以下選項的其中之一：

- 未被排程 — 只有當使用者要求時，這些任務才會被啟動。
- "一次 — 在一定的時間，只執行一次的掃描任務。在 開始日期/時間 欄位，指定開始的日期及時間。
- 週期性 — 週期地執行掃描任務，在一定的時間間隔裡(小時、天、週、月、年) 依指定的日期及時間開始進行掃描。

  在確定的時間間隔裡，如果您想要重覆某個掃描任務，請選擇 週期性 並且編輯 每一 欄位裡 minutes /hours /days / weeks/ months/ years 的數字，以指出掃描

程序的執行頻率。您必須在 開始日期/時間 欄位上指出開始執行的日期及時間 開始日期/時間 檔案

- 未被排程 — 只有當使用者要求時，這些任務才會被啟動。

按下 確定儲存變更並關閉視窗。要執行任務，請點擊掃描 。

16.2.5. 掃描物件

在您開始一個掃描程序之前，您應該先確認BitDefender 的惡意程式驗證碼是最新的。在管理主控台點擊更新>更新，可以確認是否已經擁有最新的更新。



註
為了讓 BitDefender 完成一個完整的掃描，您必須關閉所有開啟的程式。特別是電子郵件程式(如：Outlook、Outlook Express 或 Eudora) 更需要在完整掃描時進行關閉。

掃描方式

BitDefender 提供四個型態的手動掃描：

- 立刻掃描 —從系統/用戶任務進行掃瞄任務。
- 右鍵選單掃描 — 在檔案或者目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2009。
- 拖放掃描 — 拖曳一個檔案或目錄放到 掃描活動列上。
- 手動選擇掃描 — 使用BitDefender 手動選擇掃描瀏覽並選擇要掃描的檔案或檔案。

立刻掃描

要掃描您的電腦或部分，您能進行預設的掃瞄任務或您自訂的掃瞄任務 這被稱為立刻掃描。

您可以選擇以下方式的其中之一：

- 在清單要執行的任務連續點擊兩下。
- 按下所對應任務的 立即掃描 鈕。
- 選擇任務，並按下執行任務。

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 148)。

右鍵選單掃描

您可以直接使用右鍵選單直接掃描檔案或是資料夾。 右鍵選單掃描



右鍵選單掃描

在您想要掃描的檔案或目錄按下滑鼠右鍵，並選擇 BitDefender 病毒防護 2009。

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 148)。

在 右鍵選單掃描 任務的 屬性 視窗，您可以修改掃描選項並檢視報告檔案。

拖放掃描

拖放您想要掃描的檔案或資料夾到下方顯示的 掃描活動列。



拖曳檔案



放開檔案

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 148)。

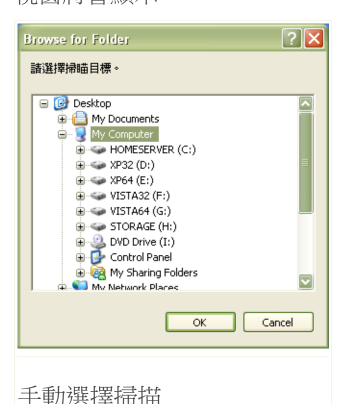
手動選擇掃描

您能夠在開始功能表中的程式集使用手動選擇掃描選項，直接瀏覽並掃描檔案。



註
手動選擇掃描是一個很方便的功能，在Windows的安全模式中也能使用。

如果您想要在開始功能表執行BitDefender掃描功能，請依照Windows 開始程式集的路徑：開始 → 程式集 → BitDefender 2009 → BitDefender 手動選擇掃描。 以下視窗將會顯示：



手動選擇掃描

選擇要掃描的物件並按下 確定。

BitDefender掃描器會立刻出現並開始掃描。 要了解更多資訊，請參考 "BitDefender 掃描器" (p. 148)。

BitDefender 掃描器

當您開始一個手動掃描程序時，BitDefender 掃描器將會出現。 依照三步驟指引執行掃描任務。

步驟 1/3 — 進行掃描

BitDefender 將會開始掃描選擇的項目。



掃瞄中

您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。



註
掃描程序將依它的複雜程度而需花費一些時間。

您可以點擊暫停，暫時停止掃描程序。點擊 回復以繼續掃描任務。

您可以點擊停止，完全停止掃描程序，而您將會直接被引導到最後的步驟。

等待BitDefender 完成掃描。

步驟 2/3 — 選擇動作。

當掃描程序完成，一個新的視窗會出現，您可以在該視窗檢視掃描結果。



動作

您可以檢視可能影響您的系統的事件數量。

被感染的物件會依照感染它們的惡意程式分組做表示。 點擊對應的威脅，您便可以得到更多關於被感染物件的資訊。

您可以針對不同的威脅類型的分組採取全體行動，也可以逐項地進行處理。

下列選項將會出現在選單中：

動作	描述
沒有採取動作	不對偵測到的檔案採取任何行動。
消毒檔案	消毒被感染的檔案。
刪除檔案	刪除所有被偵測的檔案
解除隱藏	顯示隱藏的物件。

點擊 繼續 以套用指定的動作。

步驟 3/3 — 檢視結果

當BitDefender 完成修復動作，將會出現一個掃描結果的視窗。



總結

您可以檢視結果。 顯示記錄檔案 — 檢視選擇的報告日誌。



重要
您的系統可能被要求重新啟動以完成您的清理程序。

按下 關閉 關閉視窗。

BitDefender 可能無法解決某些問題

在大部分的情形中，BitDefender 能夠成功地消毒被感染的檔案或是將之隔離。 然而，可能有極少部分的問題無法被解決。

在這種情況下，我們建議您聯絡BitDefender 在網頁www.bitdefender.com的支援團隊。 我們的技術支援代表將會協助您解決您遭遇的問題。

BitDefender 偵測到可疑的檔案

可疑的檔案是被探索式分析歸類被潛在的、沒有正式發布惡意程式碼所感染的檔案。

如果偵測到可疑的檔案，您會被要求將可疑的檔案遞交給BitDefender Lab。 點擊好將這些檔案送交BitDefender Lab做進一步的分析。

16.2.6. 檢視掃描日誌

當任務結束時，在任務按下滑鼠右鍵並選擇日誌，您可以檢視掃描結果。 以下視窗將會顯示：



掃描日誌

在此您可以檢視被執行過的任務報告。 在這裡您可以看到掃描任務被執行時，每一個時間所產生的報告檔案。當掃描被執行及掃描任務完成時，每個檔案會包含它的詳細資訊，清除/受感染、日期及時間等訊息。

有二個按鈕是可用的：

- 刪除日誌 — 刪除選擇的掃瞄日誌；
- 顯示日誌 — 檢視選擇的掃描日誌； 掃描報告將用您的預設瀏覽器開啟。



註
在檔案上按下右鍵也可以執行檢視/刪除的動作。

按下 確定儲存變更並關閉視窗。要執行任務，請點擊掃描 。

掃描日誌範例

下列表呈現一個掃描日誌的範例：



掃描日誌範例

掃描日誌包含了詳細的資訊，例如：掃描項目、掃描目標、發現的威脅與所採取的行動。

16.3. 被排除掃描的物件

當您可能需要掃描時，某些檔案會被排除。　例如，您可以要EICAR存取測試掃描或 .avi 檔案在要求時掃描。

BitDefender 允許您排除物件不被掃描，如此可以減少掃描所花費的時間以及減少對您工作的影響。

兩種能夠被排除掃描的物件：

■路徑 — 排除掃描所有在指定路徑下的檔案與資料夾。
■副檔名 — 排除掃描所有特定副檔名的檔案。



註
所有被自動掃描排除的物件將不會被掃描，無論您是否有執行。

要管理被排除掃描的物件，請在進階檢視病毒防護>例外。





例外

您可看見被排除掃描的物件。在每個物件上您可以看見它是被哪一種掃描類型排除。



註

在此，被指定的副檔名將無法使用右鍵選單掃描。

要移除項目，選擇並點擊 刪除鈕。

要編輯項目，只需選擇並點擊 編輯 按鈕或者連續按二下。 一個新的視窗將會出現，您可以在此編輯要被掃描排除的副檔名或是路徑，您也可以在此設定需要排除的掃描類型。編輯完成後，請點擊確定。



註

您也可以在物件上按下右鍵，使用右鍵功能表編輯。

在您尚未按下套用之前，可點擊 放棄 ，回復尚未儲存的設定。

16.3.1. 排除掃描路徑

要排除捷徑掃描的路徑，點擊 加入 按鈕. 一個設置精靈將會出現，並且引導您完成設定

步驟 1/4 — 選擇物件類型



物件類型

選擇要被排除的路徑選項

點擊 下一步。

步驟 2/4 — 指定要排除的路徑

BitDefender Total Security 2009

排除精靈 - 步驟 2 之 4

步驟 1 步驟 2 步驟 3 步驟 4

排除路徑
請在此輸入不要被掃瞄的路徑

瀏覽 加入

所選擇的路徑
c:\

您可以瀏覽要排除掃描的路徑，選擇排除的路徑之後請確認您已按下加入。

請謹慎選擇要被排除掃描的副檔名。爲了保護您的電腦安全，建議您不要定義任何例外的副檔名。

bitdefender 上一步 下一步 取消

排除的路徑

您可依照下列方式設定：

■按下 瀏覽，選擇要排除的檔案或資料夾並按下 加入。
■鍵入您要排除的路徑並點擊加入。



註
假如指定的路徑不存在或是出現錯誤訊息，點擊確定並檢查路徑的正確性。

當您加入路徑時，它會出現在表格中。

要移除項目，選擇並點擊 刪除鈕。

點擊 下一步。

步驟 3/4 — 選擇掃描類型

掃描類型

您會看見一個表格包含有被排除的路徑與被排除的類型。

預設中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

點擊 下一步。

步驟 4/4 — 掃描被排除的檔案



掃描被排除的檔案

強烈建議您掃描在指定路徑的檔案以確認它們沒有受到感染。 選擇此方塊在它們被排除之前先進行掃描。

點擊 完成。

按下 套用 儲存這個變更。

16.3.2. 排除掃描的副檔名

要排除指定的副檔名，請按下 ▪ 加入 按鈕。 一個設置精靈將會出現，並且引導您完成設定。

步驟 1/4 — 選擇物件類型



物件類型

選擇要排除的副檔名選項。

點擊 下一步。

步驟 2/4 — 指定的要排除的副檔名

BitDefender Total Security 2009

排除精靈 - 步驟 2 之 4

步驟 1 | 步驟 2 | 步驟 3 | 步驟 4

BitDefender 排除精靈
請在此輸入不要被掃瞄的副檔名

zip 加入

.zip (壓縮的檔案封存(archive)) 將不會被掃描

選擇副檔名

您可以選擇要排除掃描的副檔名，選擇副檔名之後請確認您已按下加入。

請謹慎選擇要被排除掃描的副檔名。爲了保護您的電腦安全，建議您不要定義任何例外的副檔名。

bitdefender 上一步 下一步 取消

要排除的副檔名

您可依照下列引導執行設定：

■從選單中選擇要排除的副檔名並且按下加入。



註
選單包含您系統所有副檔名的清單。當您選擇任何一個副檔名，您可以看見簡述(若有)。

■在編輯欄內鍵入您想排除的副檔名，並點擊加入。

當您加入副檔名時，它會出現在表格內。

要移除項目，選擇並點擊 刪除鈕。

點擊 下一步。

步驟 3/4 — 選擇掃描類型

BitDefender Total Security 2009

排除精靈 - 步驟 3 之 4

步驟 1 步驟 2 步驟 3 步驟 4

何時該套用
請選擇要套用例外的掃描類別：手動、自動、兩者。請於下表的右欄選擇適合您的選項。

所選擇的物件	何時該套用
*.zip (壓縮的檔案封存(archive))	兩者皆是

請謹慎選擇要被排除掃描的副檔名。爲了保護您的電腦安全，建議您不要定義任何例外的副檔名。

bitdefender 上一步 下一步 取消

掃描類型

您會看見一個表格包含有被排除的副檔名與被排除的類型。

預設設定中，指定的路徑是同時被自動與手動掃描排除的。 您可以點擊右邊的設定欄進行適合您的調整。

點擊 下一步。

步驟 4/4 — 選擇掃描類型



掃描類型

強烈建議您掃描指定副檔名的檔案以確認它們沒有受到感染。

點擊 完成。

按下 套用 儲存這個變更。

16.4. 隔離區

BitDefender 允許隔離受感染或可疑檔案到一個被防護的區域，名為隔離區。將這些檔案隔離在隔離區裡，會降低感染擴散的風險，同時，您也可以寄送這些檔案到 BitDefender 實驗室。

在進階檢視點擊病毒防護>隔離區，便能調整設定並管理被隔離的檔案。



隔離區

隔離區頁面顯示目前所有被隔離的檔案。 每個被隔離的檔案您可以看見它的檔名、被偵測到的病毒、原始的檔案路徑、被隔離的日期及遞交的日期



註
當病毒在隔離區中，它不能造成任何的危害，因為它們無法被執行或讀取。

16.4.1. 管理被隔離的檔案

從隔離區選擇要刪除的檔案，按下 移除 按鈕。如果您想要還原所選擇的檔案到它原始的位置，請按下 還原。

從隔離區，您可以寄送任何選擇的檔案到 BitDefender 實驗室，按下 寄送。

右鍵選單． 右鍵選單能夠讓您容易地管理隔離區。您可以選擇重新整理 更新隔離區內的項目。

16.4.2. 隔離區設定

要調整隔離區設定，按下 設定。 一個新的視窗將會開啟。



隔離區設定

您可以直接設定BitDefender執行下列動作：

刪除舊的檔案。. 要自動刪除舊的被隔離檔案，請選擇對應的項目。 您必須設定要刪除幾天以前被隔離的檔案，以及BitDefender 檢查舊檔案的頻率。



註
預設上，BitDefender會每天檢查一次並自動刪除30天以前的舊檔案。

刪除重複檔案。. 如果您想稍後才建立新的帳戶，請選擇合適的項目。 一定要指定每隔幾天再檢查重複檔案。



註
BitDefender 預設每天檢查隔離區中重複的檔案。



自動遞交檔案。. 如果您要自動遞交被隔離的檔案，請選擇合適的項目。 您必須指定遞交檔案的頻率。


註
BitDefender 預設每60分鐘一自動遞交被隔離的檔案。

更新之後掃描被隔離檔案. 如果您要自動在每次更新完成後掃描被隔離的檔案，請選取對應的項目。 點選還原無害的檔案，您可以自動地將已處理過的無害檔案還原到原始位置。

點擊 確定以儲存變更並關閉視窗。

17. 反垃圾郵件

BitDefender 反垃圾郵件雇用優異的科技創新和工業標準反垃圾郵件過濾器，當他們進入用戶的信箱之前除去垃圾郵件。

17.1. 防垃圾郵件洞察力

垃圾郵件是一個增加的問題，對個體或組織而言都是。它不漂亮，您不想要您的小孩見到它，它能使您被開除(浪費太多時間或者從接受您的辦公室郵件的色情文物)，而且您不能阻止別人傳送它。最好的方法是停止接收它。不幸地，垃圾郵件有各類型的形狀和大小，而且數量相當大。

17.1.1. 反垃圾郵件過濾器

BitDefender 反垃圾郵件引擎是由數種不同的過濾器所組成以確保收件匣沒有垃圾郵件：好友清單，垃圾郵件寄件者清單，字集過濾器，圖像過濾器, URL過濾器, 啟發式過濾器 and Bayesian過濾器。



註
您可以啟動/停用任何一個過濾器，在反垃圾郵件模組中的設定頁面。

好友清單/垃圾郵件寄件者清單

大多數的人經常與一群人溝通或者甚至接受來自相同的公司或組織網域訊息。透過使用好友或垃圾郵件寄件者清單您能容易地分類您想要接受誰(好友)的電子郵件，而不管郵件的內容為何；或者是您不想接受誰(垃圾郵件寄件者)的電子郵件。.

好友/垃圾郵件寄件者清單可以透過進階檢視或從已整合入常用的電子郵件客戶端的反垃圾郵件工具列管理。



註
我們建議您可以將好友的名稱及電子郵件位址加入好友清單。BitDefender 不會阻擋來自這些清單的郵件，因此，增加好友清單會更可以確定正常的信件可以存取。

字集過濾器

許多垃圾郵件訊息由斯拉夫或亞洲字集編寫而成。字集過濾器偵測這種訊息而且加上標籤將它們標示為垃圾郵件。

圖像過濾器

避免啟發式過濾器變得相當困難，現在的收件箱資料夾時常充滿包含一個影像的郵件。為了要應付的問題，BitDefender使用了圖像過濾器r將來自電子郵件的影像特徵與來自 BitDefender 資料庫作比較。如果一個電子郵件符合特徵將被加上垃圾郵件標籤。

URL過濾器

大多數垃圾郵件包含連結到各式各樣的網站，它可能有很多廣告並且可能是購物相關的網站，甚至有時包括網路釣魚網站。

BitDefender 維護一個含有這些連結的資料庫。 URL過濾器針對它的資料庫的一個訊息中檢查每個網址連結。如果一個訊息將被加上垃圾郵件標籤。

啟發式過濾器

啟發式過濾器在所有訊息元件上執行測試，(不只標題還有訊息本身不論是以 HTML 或文字格式)，找尋單字、詞組、連結或垃圾郵件的其他特性。 用分析的結果為基礎，為訊息計算垃圾郵件分數。

過濾器也能偵測在主題中標示 性-裸露的訊息，加上垃圾郵件標籤。



註

在 2004 年五月十九日開始，含有性行為內容的垃圾郵件一定要在主旨包含警告 性-裸露以遵守聯邦法律。

Bayesian過濾器

Bayesian過濾器模組根據統計常在垃圾郵件中出現的特定字串來區分垃圾郵件。

例如，如果某個四個字母的詞時常在垃圾郵件中出現，自然下一封出現這個詞的郵件很有可能是垃圾郵件。所有相關的字詞都會被納入計算，透過分析這些統計數據，某一個訊息是否為垃圾郵件的可能性便可以被計算出來。

這個模組呈現另一個有趣的特性：它是可訓練的。它很快適應一個特定使用者、有關的資訊收到全部的訊息的類型。若要有效地運作，過濾器一定要被訓練，要提供給它垃圾郵件和正式郵件的範本，像一隻獵犬被集中訓練追蹤一種特定的氣味。有時過濾器一定要被改正也促使調整它作出錯誤的決定的時候。



重要

您可以透過使用反垃圾郵件工具列中的 是垃圾郵件和 非垃圾郵件來修正Bayesian過濾器。



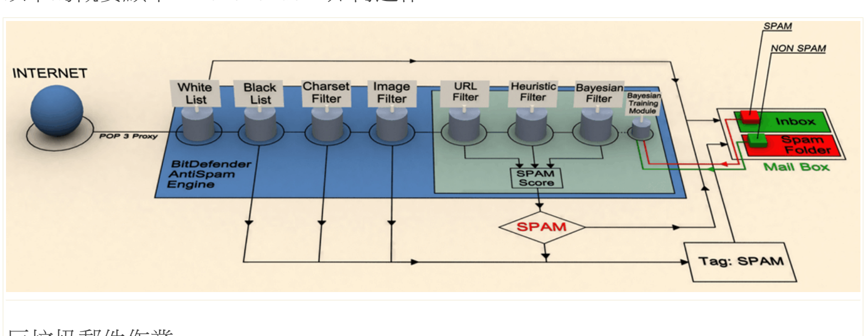
註
每一次您執行更新時：

■新的圖像特徵將會被加入到 圖像過濾器。
■新的連結將會被加入到 URL 過濾器 。
■新的規則將被加入到啟發式過濾器。

這個將會增加您的反垃圾郵件引擎的效率。
要防護您的系統以抵抗最新的垃圾郵件寄件者，請保持 自動更新啟動。

17.1.2. 反垃圾郵件作業

以下的概要顯示 BitDefender 如何運作。



反垃圾郵件作業

反垃圾郵件過濾器從上述的概要 （好友清單，垃圾郵件寄件者清單，字集過濾器，圖像過濾器，URL過濾器，啟發式過濾器以及 Bayesian過濾器)一起用於BitDefender的反垃圾郵件模組中，決定一封特定郵件是否應該到您的收件匣。

來自網際網路的每份電子郵件首先檢查好友清單/垃圾郵件寄件者清單過濾器。如果寄件人的地址在好友清單被發現電子郵件會被直接移動到收件匣。

否則，垃圾郵件寄件者清單過濾器將會處理該郵件，這封郵件將會被標為垃圾郵件並且被移至垃圾郵件資料夾(位於 Microsoft Outlook)。

另外，字元過濾器 將檢查電子郵件是否以斯拉夫語系或亞洲語系所寫。如果是，則電子郵件將在主旨加上 [垃圾郵件]，並移到 垃圾郵件資料夾。

如果電子郵件不是以斯拉夫語系或亞洲語系所寫，則將進行 圖像過濾器。這個 圖像過濾器 將偵測電子郵件所附加的圖像，是否含有垃圾郵件的內容。

URL過濾器 將會檢查連結並與 BitDefender 資料庫進行比對。如果找到相符合的，則將在這封電子郵件增加垃圾郵件的分數。

那 啟發式過濾器 將接管電子郵件而且將所有的訊息內容進行一組測試，找尋字、詞組、連結或垃圾郵件的其他特性。結果是將在這封電子郵件增加垃圾郵件的分數。



註
如果電子郵件被附以標籤，如含有性-裸露的在主題中，BitDefender 將視它為垃圾郵件。

這Bayesian過濾器 模組將更進一步分析訊息，根據常出現在垃圾郵件中的字詞統計資訊，將在這封電子郵件增加垃圾郵件的分數。。

如果一個訊息合計得分 (URL得分+啟發得分+Bayesian得分) 超過使用者在 狀態設定的層級，訊息被視為垃圾郵件。



重要
如果您不是使用 Microsoft Outlook 或 Microsoft Outlook Express 的電子郵件客戶端，您應該建立一個規則，若電子郵件主旨含有[SPAM]則移到一個自訂的隔離資料夾。BitDefender 會在判定的垃圾郵件上附加 [SPAM] 在主旨欄位。

17.2. 狀態

若要配置反垃圾郵件防護，請在進階檢視選擇反垃圾郵件>狀態。



反垃圾郵件狀態

您可以在此檢視反垃圾郵件是啟動或已停用。 如果您想變更反垃圾郵件狀態，請選取或清除對應的核取方塊。



重要
要防止垃圾郵件進入您的 收件匣，請保持 反垃圾郵件過濾器啟動。

在 統計 頁面，您可以檢視反垃圾郵件活動的狀況 (從您啟動您的電腦後) 或總結 (從您安裝 BitDefender 後)。

17.2.1. 設定保護層級

您可以選擇最適合您安全需求的防護層級。拖曳滑桿設定合適的防護層級。

有五種防護層級：

防護層級	描述
寬鬆	針對接收到大量合法商業信件的電子郵件帳號提供防護。過濾器將會讓多數的電子郵件存取，但它可以產生誤判情形（垃圾郵件被歸類於合法的郵件）。
寬鬆到中等	針對接收到一些合法商業信件的電子郵件帳號提供防護。過濾器將會讓多數的電子郵件存取，但它可以產生誤判情形（垃圾郵件被歸類於合法的郵件）。
中等	針對一般電子郵件帳號提供防護。 過濾器將封鎖多數的垃圾郵件，避免誤判情形。
中等到嚴謹	針對接收到大量垃圾郵件的電子郵件帳號提供防護。 過濾器將讓少量的垃圾郵件存取，但它可能產生誤判（正常的郵件被標示為垃圾郵件）。 設置好友/垃圾郵件寄件者清單 並訓練 學習引擎(Bayesian)以減少誤判的數量。
嚴謹	針對接收到非常大量垃圾郵件的電子郵件帳號提供防護。過濾器將讓少量的垃圾郵件存取，但它可能產生誤判(正常的郵件被標示為垃圾郵件)。 加入您的聯絡人到 好友清單以減少誤判的數量。

要使用預設的防護（中等到嚴謹），點擊 預設層級。

17.2.2. 設置好友清單

好友清單是您所有想要接受的電子郵件位址清單，不管它們的內容為何。從您的好友寄來的郵件都不會被列為垃圾郵件，即使它的內容類似垃圾郵件。



註
任何列於 好友清單 的電子郵件，都會自動地傳送到您的收件匣而不需進行處理。

要設置好友清單，點擊管理好友（或點擊反垃圾郵件工具列的 好友鈕。



好友清單

在這裡，您可以從 好友清單 加入或刪除內容。

如果您想要新增一個電子郵件位址，勾選 電子郵件位址 選項，輸入位址並點擊 ⊡。這個位址將會出現在 好友清單。



重要
語法：name@domain.com。

如果您想要新增一個網域，勾選 網域名稱 選項，輸入網域名稱並點擊 ⊡。這個網域名稱將會出現在 好友清單。



重要
語法：

- @domain.com、*domain.com 及 domain.com — 所有從 domain.com 接收到的電子郵件訊息都將直接傳到您的 收件匣 不管它們的內容為何；
- *domain* — 所有從 domain(不管網域的語法) 接收到的電子郵件訊息都將直接傳到您的 收件匣 不管它們的內容為何；
- *com — 所有接收到的電子郵件以 com 為字尾，都將直接傳送到您的 收件匣 不管它們的內容為何；

要刪除清單中的一個項目，選擇它並點擊 移除 按鈕。如果您點擊 清除清單 按鈕，您將刪除清單中所有的內容，請注意：刪除後不可能再回復它。

使用 儲存/ 載入 按鈕去儲存/載入 好友清單 到需要的位置。這個檔案以 .bwl 為副檔名。

當您載入一個先前儲存的清單，選擇 當載入時，清空目前的清單，則目前的清單即會被重新清除。



註
我們建議您可以將好友的名稱及電子郵件位址加入好友清單。BitDefender 不會阻擋來自這些清單的郵件，因此，增加好友清單會更可以確定正常的信件可以存取。

點擊 套用 及 確定以儲存並關閉 好友清單。

17.2.3. 設置垃圾郵件寄件者清單

垃圾郵件寄件者清單 是一個電子郵件位址清單，它包含您不想接受到的郵件，不管它的內容為何。



註
任何來自 垃圾郵件寄件者清單 的電子郵件，都將自動地被標示為垃圾郵件，不需要進行處理。

要設置垃圾郵件寄件者清單，點擊管理垃圾郵件寄件者 (或點擊反垃圾郵件工具列的 垃圾郵件寄件者鈕。



垃圾郵件寄件者清單

在這裡您可以從 垃圾郵件寄信者清單 加入或刪除內容。

如果您想要新增一個電子郵件位址，勾選 電子郵件位址 選項，輸入位址並點擊 。這個位址將出現在 垃圾郵件寄信者清單。



重要

語法：name@domain.com。

如果您想要新增一個網域，勾選 網域名稱 選項，輸入網域並點擊 。這個網域名稱將出現在 垃圾郵件寄信者清單。



重要

語法：

- @domain.com、*domain.com 及 domain.com — 所有從 domain.com 接收到的電子郵件都將被標示為垃圾郵件；
- *domain* — 所有從 domain（不管網域的字尾為何）接收到的電子郵件都將被標示為垃圾郵件；
- *com — 所有接收到以 com 為網域字尾的電子郵件都將被標示為垃圾郵件。

要刪除清單中的一個項目，選擇它並點擊 移除 按鈕。如果您點擊 清除清單 按鈕，您將刪除清單中所有的內容，請注意：刪除後不可能再回復它。

使用 儲存/ 載入按鈕去儲存/載入 垃圾郵件寄件者清單到需求的位址。這個檔案將以 .bwl 為副檔名。

當您載入一個先前儲存的清單，選擇 當載入時，清空目前的清單，則目前的清單即會被重新清除。

點擊 套用及 確定以儲存並關閉 垃圾郵件寄件者清單。



重要
如果您想要重新安裝 BitDefender，建議先儲存 好友 / 垃圾郵件寄件者 清單，在完成重新安裝程序後，您可以再載入它們。

17.3. 設定

要設置反垃圾郵件設定及過濾器，請在進階檢視選擇反垃圾郵件>設定。



反垃圾郵件設定

這個選項有三種可用的類型 (反垃圾郵件設定、基本的反垃圾郵件過濾器 及 進階的反垃圾郵件過濾器) 它們以可展開的選單方式呈現，類似於 Windows 介面。



註

點擊 "+" 號方塊展開種類， "-" 號方塊關閉。

要啟動/關閉選項，請選取/清除相對應的核取方塊。

要套用預設設定，點擊預設。

按下 套用 儲存這個變更。

17.3.1. 反垃圾郵件設定

■在主旨標示垃圾郵件 — 所有被視為垃圾的電子郵件都將在主旨列加上 SPAM。

■在主旨標示釣魚郵件 — 所有被視為釣魚的電子郵件都將在主旨列加上 SPAM。

17.3.2. 基本的反垃圾郵件過濾器

■好友/垃圾郵件寄件者清單—透過好友/垃圾郵件寄件者清單過濾郵件。
- 自動加入收件者到好友清單 — 在傳送郵件時，自動加入收件者到好友清單。
- 自動地加入到好友清單— 下一次您從 反垃圾郵件工具列 點擊 非垃圾郵件 按鈕，則寄件者將自動新增到 好友清單。
- 自動地加入到垃圾郵件寄件者清單 — 下一次您從 反垃圾郵件工具列 點擊 垃圾郵件 按鈕，則寄件者將自動新增到 垃圾郵件寄件者清單。



註
這個 非垃圾郵件 及 垃圾郵件 按鈕，是使用來訓練 Bayesian過濾器。

■封鎖亞洲語系 — 封鎖以 亞洲字元所寫的電子郵件。

■封鎖斯拉夫語系 — 封鎖以 斯拉夫字元 所寫的電子郵件。

17.3.3. 進階的反垃圾郵件過濾器

■啟動Bayesian學習引擎 — 啟動/關閉 Bayesian學習引擎。
- 限制字典大小為 200000 字 — 設定Bayesian字典檔大小，小一點掃描速度會快一些，而大一點則較精確。



註
建議大小為：200,000 字。

- 針對外傳的郵件訓練學習引擎(Bayesian) — 對於外傳的電子郵件，訓練學習引擎。

■URL過濾器 — 啟動/關閉 URL過濾器。

■啟發式過濾器 啟動/關閉 啟發式過濾器。
- 封鎖裸露內容 — 啟動/關閉偵測在郵件主旨裡含有性-裸露內容的訊息。

■圖像過濾器 — 啟動/關閉 圖像過濾器。

18. 家長管控

BitDefender 家長管控讓您能夠管控系統中每一個帳號存取網際網路以及特定應用程式。

您可以設置家長管控要阻擋的項目：

■不適當內容的網路頁面。

■在特定時間存取網際網路.(例如課業時間) 。

■含有關鍵字的網頁及電子郵件將會被阻擋。

■如遊戲、聊天、檔案分享程式或其他應用程式。

■除了允許的聯絡人之外傳送的即時訊息。



重要

只有具有系統管理權限的使用者才存取與設置家長管控。 您可以設定家長管控密碼，以防止他人更改設定。 當您針對某使用者啟動家長管控時，需要輸入密碼。

要成功使用家長管控以限制您的孩子電腦與網路活動，您需要完成這些任務：

1.建立受限制的(標準的)Windows使用者帳戶讓您的孩子使用。



註

要了解如何建立Windows使用者帳戶，請至Windows說明與支援中心(於開始功能表點擊說明與支援)。

2.為孩子使用的Windows使用者帳戶設置家長管控。

要設定家長管控，請在進階檢視進入家長管控。

家長管控

您可以看到家長管控在每一個Windows使用者帳戶設置功能的狀態。 雙擊一個使用者名稱以開啟視窗，您可以在視窗中設置家長管控。

此章節以下的部分將詳細說明家長管控的特色與設置方法。

18.1. 設定每一個使用者的狀態

要設置家長管控，請雙擊使用者對象並點擊狀態標籤。



家長管控狀態

要設置這個使用者帳戶的家長管控，請依照以下步驟：

1. 選取家長管控方塊以啟動此使用者帳戶的家長管控。



重要

保持家長管控啟動，可以使用您自訂的電腦存取規則，保護您的兒童遠離不正當的網頁內容。

2. 設定密碼以保護您的家長管控設定。 要了解更多資訊，請參考 "家長管控設定" (p. 182)。

3. 選取方塊對應您想使用的保護。

■網站管控 - 根據您在網站頁面的設定，啟動網站管控以過濾網站的瀏覽。

■應用程式管控 - 依據您在 應用程式頁面的設定，啟動 應用程式管控 以阻擋特定應用程式存取。

■即時通訊管控 - 依據您在 即時通訊傳輸頁面的設定，允許或阻擋即時交談訊息。

■網頁時段限制器 - 根據您在 時段控制工具頁面的設定，允許存取網頁。

■網站存取 -阻擋所有網站的存取(不僅網站頁面的內容)。

■關鍵字過濾器 - 根據您在關鍵字頁面設定的規則，過濾網頁、電子郵件與即時通訊。

■啟發式網站過濾器 -根據先前定義的年齡分類規則過濾網站存取。

4. 為了發揮家長管控的功能，您必須設置一些管控設定。 要了解如何設置這些設定，請參照下面的主題。

18.1.1. 家長管控設定

如果您不是此電腦唯一擁有管理權限的人，建議您設定密碼保護您的家長管控設定。設定一個密碼，您可以阻止其他使用者變更您對特定使用者設置的家長管控設定。

當啟動家長管控時， BitDefender將預設詢問您是否設定一組密碼。

BitDefender家長管控 – 密碼

要確保只有您能夠變更家長管控設定，我們建議您使用密碼保護這個模組。預設上，這只保護家長管控模組，但您能在進階設定視窗變更其他相關設定保護。

您想現在設定密碼嗎?

密碼

重新輸入密碼

密碼長度應至少為 8 個字元。

☐當啓動家長管控時不要詢問密碼。

確定 取消

設定密碼防護

若要設定密碼保護，如下：

1. 在密碼欄位輸入密碼。

2. 在重新輸入密碼欄位再次輸入密碼。

3. 點擊確定儲存密碼並關閉視窗。

當您設定密碼後，變更家長管控設定需要密碼。 如果有其他的系統管理員要改變家長管控設定，也必須輸入密碼。



註
這密碼不會使用在保護其他 BitDefender 設定。

若您不想使用密碼保護，可以選取啟動家長管控時不要求密碼。

18.1.2. 設置啟發式網站過濾

啟發式網站過濾器分析並阻擋可能含有不適當內容的網頁。

若要根據預先設定的年齡規則過濾網頁，您必須先選擇一個容許層級。 拖曳滑桿至您認為適合這個使用者的容許層級。

有3種容許層級：

容許層級	描述
兒童	提供網站存取的限制，依據 14 歲以下使用者的建議設定值。網頁中可能包含對幼童有害的內容(色情的、藥物的、暴力攻擊等) 都將被封鎖。
青少年	提供網站存取的限制，依據 14 到 18 歲使用者的建議設定值。包含有色情或成人內容的網頁會被封鎖。
成年人	提供無限制的網站存取，不管網站的內容為何。

點擊預設層級設定滑桿在預設層級。

18.2. 網站管控

網站管控幫助您阻擋含有不適當內容的網站。BitDefender 提供阻擋網站的清單，這也是定期更新的一部份。

要設置網站管控，請雙擊使用者並點擊網站標籤。

網站管控

要啟動這個防護，選取啟動網站管控方塊。

選擇允許存取這些網頁/阻擋存取這些網頁以檢視允許/阻擋的網站清單。點擊例外...您可以設定例外清單。

規則可以手動輸入。首先，選擇 允許存取這些網頁/阻擋存取這些網頁以允許/阻擋您指定的網站存取。然後點擊 新增...鈕以啟動設置精靈。

要刪除一個規則，選擇它並點擊 刪除鈕。要更改一個規則，選擇它並點擊 編輯...鈕或雙擊規則。若只是暫時不啟動規則，只需取消勾選。

按下 套用 儲存這個變更。

18.2.1. 設置精靈

設置精靈只有一個步驟。

步驟 1/1 - 指定網站

BitDefender 2009 - 網站精靈

輸入URL

您可以輸入單一網頁位址或包含萬用字元的網址。

例如：您可以輸入 *cigars* 來阻擋所有包含cigars的位址。

完成 取消

指定網站

輸入套用規則的網站，並點擊完成。



重要

語法：

- *.xxx.com - 這個規則將被套用在所有網址以 .xxx.com 結尾的網站；
- *porn* - 這個規則將被套用在網址中包含 porn 字串的網站；
- www.*.com - 這個規則將被套用在網址以 com 為字尾的網站；
- www.xxx.* - 這個規則將被套用在網址以 www.xxx.開頭的網站，不管它的字尾是什麼。

18.2.2. 指定例外

有時候您為套定規則指定例外。例如，當您設定規則封鎖包含有 "killer" 網址的網站 (語法：*killer*)，但您想存取一個叫做 killer-music的線上音樂網站。要在先前建立好的規則建立一個例外，請進入例外 視窗，並定義例外規則。

點擊例外...。以下的視窗將會出現：

指定例外

點擊新增...以指定例外。設置精靈 將會出現。完成這個精靈以設定例外。

要刪除一個規則，選擇它並點擊刪除。要更改一個規則，選擇它並點擊編輯或雙擊規則。若只是暫時不啟動規則，只需取消勾選。

點擊 關閉以儲存變更並關閉視窗。

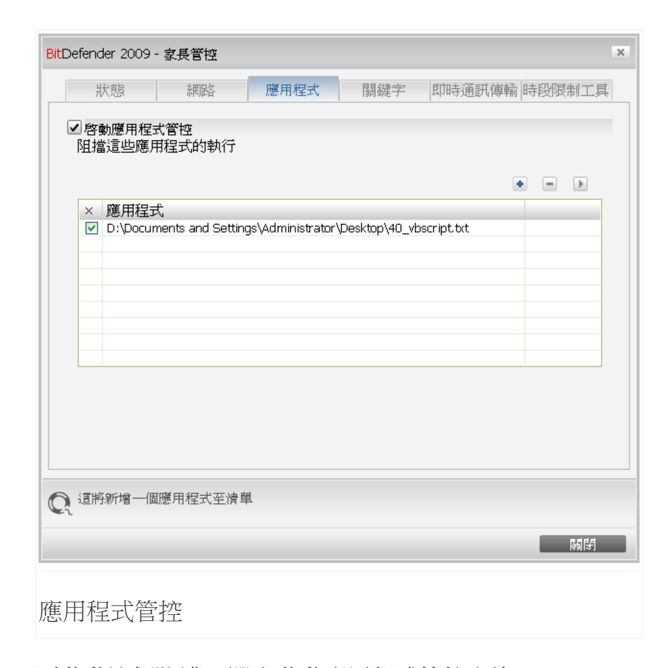
18.2.3. BitDefender 網站黑名單

為了協助您保護您的孩子，BitDefender 提供不適當或危險的網站黑名單。要封鎖網站選擇 使用 BitDefender 所提供的網站封鎖清單。

18.3. 應用程式管控

應用程式管控協助您阻擋任何應用程式。遊戲、多媒體、即時傳訊軟體等及惡意程式也可以利用這種方式阻擋。透過這種方式被阻擋的應用程式也受到修改的保護，並且無法被複製或移動。

要設置應用程式管控，請雙擊使用者並點擊應用程式標籤。



應用程式管控

要啟動這個防護，選取啟動應用程式管控方塊。

規則必須手動輸入。點擊 新增...鈕，以開啟設置精靈。

要刪除一個規則，選擇它並點擊 刪除鈕。要更改一個規則，選擇它並點擊 編輯...鈕或雙擊規則。若只是暫時不啟動規則，只需取消勾選。

按下 套用 儲存這個變更。

18.3.1. 設置精靈

設置精靈只有一個步驟。

步驟 1/1 - 選擇要封鎖的應用程式

BitDefender 2009 - 應用程式精靈

輸入應用程式名稱

瀏覽(B)

點擊[瀏覽]選擇程式檔案。

重要：用這個方法封鎖的檔案同時受到修改保護，也無法被複製或搬移。

加入應用程式至這個清單以預防它們被存取

完成 取消

選擇要封鎖的應用程式

點擊瀏覽，選擇要封鎖的應用程式並點擊完成。

18.4. 關鍵字過濾

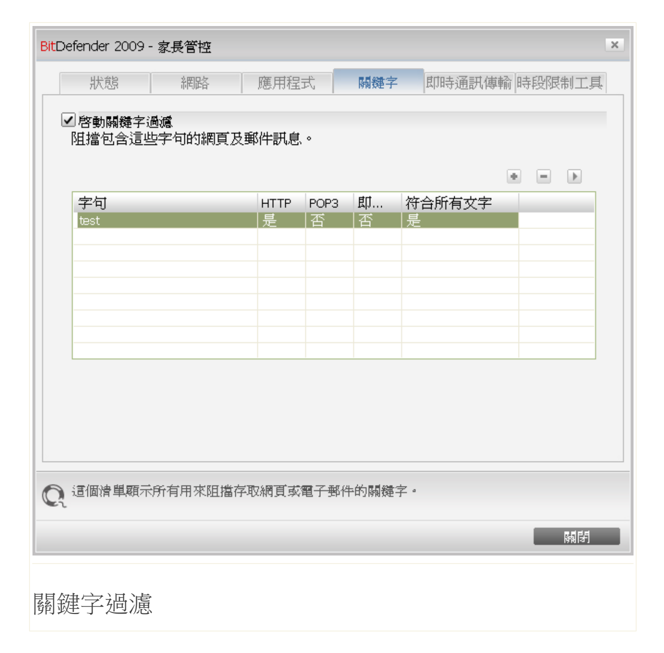
關鍵字過濾幫助您阻擋包含特定字句的電子郵件、網頁和即時訊息的存取。 使用關鍵字過濾器，您可以防止您的孩子在網路上看到不適當的字句內容。



註

即時訊息關鍵字過濾器可以用在Yahoo即時通和Windows Live (MSN) Messenger。

要設置關鍵字過濾器，請雙擊使用者並點擊關鍵字標籤。



關鍵字過濾

若您想使用此功能，請選擇 啟動關鍵字過濾器選取方塊。

您必須加入要阻擋的關鍵字規則。 要加入規則，請點擊 加入鈕並在設置視窗中輸入規則參數。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要編輯現有規則，請雙擊規則或點擊 編輯鈕，並在設置視窗中更改規則。

按下 套用 儲存這個變更。

18.4.1. 設置視窗

當您加入或編輯規則，設置視窗將出現。

輸入關鍵字

您必須設定以下的參數：

- 關鍵字 - 在編輯欄位輸入您想要封鎖的字元或段落。
- 通訊協定 - 選擇 BitDefender 應該掃描指定字元的通訊協定。

選項	描述
POP3	含有關鍵字的電子郵件將會被封鎖。
HTTP	含有關鍵字的網頁將會被封鎖。
即時訊息	含有關鍵字的即時訊息將會被封鎖。

點擊完成 以加入規則。

18.5. 即時通訊管控

即時通訊管控提供您指定您的孩子允許交談的連絡人。





註
即時通訊管控只適用於Yahoo即時通和Windows Live (MSN) Messenger。

要設置即時通訊管控，請雙擊使用者並點擊即時通訊傳輸標籤。



即時通訊管控

若您想使用此功能，請選擇 啟動即時通訊管控選取方塊。

您必須加入規則以指定該使用者被允許或不允許交談的聯絡人。 要加入規則，請點擊 加入鈕並在設置視窗中輸入規則參數。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要編輯現有規則，請雙擊規則或點擊 編輯鈕，並在設置視窗中更改規則。

若您已定義允許交談的聯絡人，您可以選擇阻擋所有不在此清單的即時通訊使用者。 這樣，只有已指定允許的聯絡人可以傳送即時訊息給該使用者。

按下 套用 儲存這個變更。

18.5.1. 設置視窗

當您加入或編輯規則，設置視窗將出現。

BitDefender 2009 - 即時通訊精靈

在這裡輸入您想加入至限制清單的連絡人名稱

testauto@live.com

選擇即時通訊程式類型

MSN Live Messenger

動作

○ 拒絕與這個聯絡人交談

◉ 允許與這個聯絡人交談

加入一個您允許或拒絕交談的即時通訊聯絡人

點擊這裡允許包含指定內容的即時訊息

完成 取消

加入即時通訊聯絡人

步驟如下：

1. 輸入聯絡人的使用者名稱(ID)。
2. 選擇該聯絡人的即時通訊程式。
3. 選擇一個規則動作：
   - 拒絕與此聯絡人交談
   - 允許與此聯絡人交談
4. 點擊完成 以加入規則。

18.6. 網路時段限制器

網路時段限制器協助您在指定的時段允許或封鎖使用者或應用程式存取網路。



註
但無論網路時段限制器的設定為何，BitDefender 都將每小時執行更新。

要設置網路時段限制器，請雙擊使用者並點擊網路時段限制器標籤。



網路時段限制器

要啟動這個防護，選取啟動網路時段限制器方塊。

選擇封鎖所有網際網路連線的時段。您可以點擊方格選取單一時段、或是拖曳選取長時段。您也可以點擊全部選取以選取全部的方格，阻擋所有網路存取。如果您點選取消選取全部，表示在任何時間都允許網路連線。



重要
灰色的方格代表封鎖網際網路存取的時段。

按下 套用 儲存這個變更。



19. 隱私權管控

BitDefender監控您的系統中多處可能受間諜程式攻擊的熱點，並檢查您的系統和軟件的異動。這是有效封鎖木馬程式及其他駭客安裝的工具程式，駭客會試圖竊取您的個人資料（如：信用卡號碼等）並寄送出去。

19.1. 隱私權管控狀態

要設置隱私權管控以及檢視其活動，請在進階檢視中進入隱私權管控>狀態。



隱私權管控狀態

您可以看到隱私權管控是啟動或停用。 如果您想更改隱私權管控狀態，請選取或取消選取對應的方塊。



重要

為了防止資料遭竊並保護您的隱私，請持續保持啟動隱私權管控。

隱私權管控使用這些重要防護管控來保護您的電腦：

- 身分管控 - 根據您在 身分頁面建立的規則，對外的網頁(HTTP)及電子郵件(SMTP)傳輸都會被過濾，以保護您的機密資料。
- 登錄管控 - 當有程式進入開始功能表執行而嘗試修改登錄項目時，先徵求您的同意。
- Cookie管控 - 當一個新的網站嘗試設定一個 cookie時，先徵求您的同意。
- Script管控 - 當一個網站嘗試啟動一個script或其他內容時，先徵求您的同意。

在頁底您可以看到身分管控統計資料。

19.1.1. 設置防護層級

您可以選擇最適合您安全需求的防護層級。拖曳滑桿設定合適的防護層級。

有三種防護層級：

防護層級	描述
寬鬆	只有登錄管控已啟動。
預設	登錄管控及身分管控 已啟動。
嚴謹	登錄管控、身分管控 及 Scrpit管控已啟動。

您可以點擊自訂層級以自訂防護層級。 在出現的視窗中，選擇您要啟動的防護管控並點擊確定。

點擊預設層級，將滑桿拖曳至預設層級。

19.2. 身分管控

保持機密資料的安全是個重要的議題。在網際網路的發展下，資料竊盜技術也隨之進步，它利用一些新的方法來騙取人們提供個人私密的資料。

不管是您的電子郵件或您的信用卡號碼，當落入壞人的手中，絕對會造成您重大的損失：您會發現您的信箱被垃圾郵件所淹沒，或是您將會絕望的面對一個掏空的銀行帳號。

身分管控能夠保護您在線上時免於被竊取敏感的資料。 根據您所建立的規則，身分管控將會掃描從網頁、電子郵件或即時通訊中有沒有出現特定字串(例如：信用卡號碼)。如果掃描到特定字串，該網頁、電子郵件或即時通訊將會被阻擋。

您可以建立規則以保護您的所有個人隱私資料，例如手機號碼、電子郵件位置，亦或是銀行帳戶資訊。 提供多使用者服務，不同的Windows使用者帳戶可以設置自己的身分保護規則。 您建立的規則只在您登入您的Windows使用者帳戶時才會套用並存取。

為什麼要使用身分管控？

- 身分管控對於阻擋鍵盤記錄的間諜程式非常有效。 這種惡意程式會紀錄您的鍵盤打字記錄，並利用網路傳送給駭客。 駭客可以藉此得到您的敏感資訊，例如銀行帳戶號碼、密碼，並使用它得利。

  只要您建立了恰當的身分防護規則，即使間諜程式成功避開病毒防護的檢查，仍無法以電子郵件、網頁或即時訊息的方式傳送被偷取的資料。

- 身分管控能保護您不受網路釣魚企圖。(企圖偷取您的個人資訊)。 最常見的網路釣魚使用假郵件，讓您進入假的網頁輸入個人資訊。

  例如，您可能收到一封聲稱來自銀行的郵件，要求您緊急更新您的銀行帳戶資訊。這封郵件給您一個網頁連結，並要求你輸入個人資料。 即使郵件與網頁看似正常，其實它們都是假的。 如果您點擊了郵件中的連結、並在網頁中輸入您的個人資料，您將揭露這些資訊給網路駭客。

  如果您已設置恰當的身分防護規則，您就無法遞交個人資訊(例如您的信用卡號)至一個您未定義成例外的網頁。

要設置身分管控，請在進階檢視中進入隱私權管控>身分。



身分管控

如果您想要使用身分管控，請依照以下步驟：

1. 選擇身分管控選取方塊。
2. 建立規則以保護您的敏感資料。 要了解更多資訊，請參考"建立身分管控規則" (p. 197)。
3. 如果有需要，在您所建立的規則中定義特定的例外。 要了解更多資訊，請參考"定義例外規則" (p. 201)。

19.2.1. 建立身分管控規則

要建立身分保護規則，請點擊 加入鈕並依照設置精靈進行。

步驟 1/4 - 歡迎視窗

BitDefender 2009 - 身分規則精靈

身分管控模組能夠監控HTTP(網站)和SMTP(郵件)的傳輸，以防您的私密資訊，例如：信用卡號碼、身分證字號或其他用戶定義的字串(例如：密碼的一部分)，透過網路流出。

這個精靈將引導您建立所需的身分管控規則。您也可以在身分管控標籤中點擊新增規則的圖示，進階檢視>隱私權管控來設定。

下一步 取消

歡迎視窗

點擊 下一步。

步驟 2/4 - 設定規則類型及資料

BitDefender 2009 - 身分規則精靈

規則名稱

規則種類 名字

規則資料

個人資料已被加密並無法被除了您以外的任何人使用。爲了額外的安全，請輸入部份您要保護的資料。(例如:如果您想過濾傳送至電子郵件位址:john.doe@example.com,您應該只包含"john"

請在這裡輸入規則名稱

上一步 下一步 取消

設定規則類型及資料

您必須設定以下的參數：

■規則名稱 — 在編輯欄位中輸入規則的名稱。

■規則類型 — 選擇規則類型（住址、姓名、信用卡號碼、身分證號碼等)。

■規則資料 —在編輯欄位中輸入您想要保護的資料。 舉例來說，如果您想保護您的信用卡號碼，在這裡輸入全部或部分的號碼。



註

如果您輸入少於三個字元，您將會被提示驗證資料。我們建議您最少三個字元以避免被阻擋錯誤發生。

在這裡您所輸入的資料都會被加密。為了加強安全性，請不要輸入完整的資料。

點擊 下一步。

步驟 3/4 - 選擇傳輸方式

BitDefender 2009 - 身分規則精靈

☑掃描 HTTP
☐掃描 SMTP
☑掃描即時訊息

☑符合所有文字
☐符合事件

HTTP(網路)傳輸 與 即時通訊傳輸 containing your personal information will be blocked.

選取以啟動掃描網站(HTTP)傳輸

上一步 下一步 取消

選擇傳輸方式

選擇您希望BitDefender掃描的傳輸方式： 以下的選項是可用的：

- 掃描 HTTP — 掃描 HTTP(網站) 傳輸，並阻擋符合規則的外送資料。
- 掃描 SMTP — 掃描 SMTP(電子郵件) 傳輸，並封鎖符合規則的外送電子郵件。
- 掃描即時通訊 — 掃描即時通訊傳輸，並封鎖符合規則的外送即時訊息。

您可以選擇在整個單字符合規則資料時套用規則，偵測到的字串事件相符時套用規則。

點擊 下一步。

步驟 4/4 - 規則描述

規則描述

在編輯的欄位上輸入一個規則的簡短描述。 由於存取規則時，被阻擋的資料(字串)不會顯示，所以述能幫助您分辨規則。

點擊 完成。 規則將出現在表中。

19.2.2. 定義例外規則

這是您可能須要對特定的身分規則定義例外的情況。 當您真的需要將您的信用卡資料藉由網路傳送遞交時，您可以設定規則的例外。

要管理例外規則，點擊 例外 。

例外

要加入例外，請依照下列步驟：

1. 點擊加入在表格裡加入新的項目。
2. 雙擊指定允許的位址　，輸入您要加入例外的網址、電子郵件位址或即時通訊連絡人。
3. 點擊兩下選擇類型並從選單選擇對應的您輸入的資料選項。
   - 如果您指定了一個網址，請選擇HTTP。
   - 如果您指定了一個電子郵件地址，請選擇SMTP。
   - 如果您指定了一個即時通訊連絡人，請選擇即時通訊。

從例外清單裡選擇並點擊移除即可移除不用的例外項目。

點擊確定 以儲存變更。

19.2.3. 管理規則

您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。

要編輯一個規則，只需點選規則並點擊 編輯 鈕，或雙擊規則，一個新的視窗即會出現。



編輯規則

您可以在這裡變更規則的名稱、描述及參數(種類、資料及掃描傳輸的方式)。點擊確定 儲存設定。

19.3. 登錄管控

登錄鍵 在 Windows 作業系統是一個非常重要的部份。這是 Windows 放置設定、安裝的程式、使用者資訊等相關重要設定的地方。

登錄鍵　也被使用來定義哪個程式在Windows啟動時自動執行。當使用者重新啟動電腦時，病毒也常利用這個方式自動啟動。

登錄管控監控Windows 登錄鍵的變化 - 這是偵測木馬程式有效的方法。每當程式試著修改登錄鍵，以便在 Windows 啟動時被執行時，它將會先警告您。



登錄警示

您可以看到正試圖更改Windows登錄鍵的程式。

若您無法辨識此可疑的程式，點擊阻擋以避免其更改Windows登錄鍵。 或者點擊允許以允許其更改。

根據您的回應，將建立一個規則並列於規則表格中。 若此程式再次要求更改登錄鍵，將自動套用相同的行動。



註

當您安裝新的程式且必須在下次系統啟動時執行，BitDefender將會提示您。多數情形下，這些程式是合法且可被信任的。

要設置登錄管控，請在進階檢視中進入隱私權管控>登錄。



登錄管控

您可以在表格中檢視目前已建立的規則清單。

要刪除一個規則，只需點選規則並點擊 刪除鈕。

19.4. Cookie 管控

Cookies 是網際網路上一個常見的記錄。它是存在您電腦裡非常小的一些檔案。網站透過建立這些 cookies 以保持您的追蹤資訊。

Cookie 讓您的生活變得更方便。舉例來說，它們可以讓網站記住您的名字及相關的資訊，所以，您不需要每次造訪網站時都重新輸入這些資訊。

但透過追蹤您的記錄樣本，cookies也可能被利用洩露您的隱私資料。

Cookie管控能夠幫助您，在您啟動 Cookie管控時，新的網站試圖設定一個cookie將先徵求您的同意：



Cookie警示

您可以看見正試圖寄送cookie檔案的應用程式名稱。

點擊記住這個答案 選項，並點擊 是 或 否，建立並套用規則，並列於表格裡。當您下次再連線到相同的網站時，您將不再被提示。

這將協助您選擇哪個網站您要信任或不信任。



註

現今大量的cookie被使用在網際網路上，所以Cookie 管控 一開始使用可能有點麻煩。首先，當網站試圖儲存 cookie 在您的電腦時，它將詢問一些問題。很快地，您新增常造訪的網站到規則清單裡，它將變得越來越方便。

要設置Cookie管控，請在進階檢視中進入 隱私權管控>Cookie。

BitDefender 網路安全 2009 - 試用　切換到基本檢視

狀態：有3個需留意的事件　修復所有事件

狀態　身分　登錄　Cookies　Script

一般
病毒防護
反垃圾郵件
家長管控
隱私權管控
防火牆
系統弱點
加密
遊戲/筆電模式
網路
更新
註冊

啟動Cookie管控
Cookies已阻擋：　0

網域	方向	動作	

選取這個方塊以啟動Cookie管控。Cookies可能被用來追蹤網站瀏覽紀錄，建議您勿接受不信任網站的Cookie。

bitdefender　購買 - 我的帳號 - 註冊 - 說明 - 支援 - 歷史

Cookie 管控

您可以在表格中檢視目前已建立的規則清單。



重要

規則將依序它們的優先權由上而下排列，越高就越優先。拖曳這些規則以更改他們的優先權。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要更改這些規則參數，雙擊規則並在設置視窗中更改。

要手動增加規則，點擊 加入鈕並在視窗中設置規則參數。

19.4.1. 設置視窗

當您編輯或手動加入一個規則時，設置視窗將出現。

選擇位址、動作及方向

您可以設置參數：

■網域位址 - 在規則裡，輸入所應套用的網域。
■動作 - 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 cookie 將會被執行。
拒絕	在這個網域的 cookie 將不會被執行。

■方向 - 選擇傳輸的方向。

類型	描述
外傳	這個規則只套用在被傳送到連線網站的 cookies。
接收	這個規則只套用在從連線網站所接收的 cookies。
兩者皆是	這個規則套用到進出二個方向。



註
您可以接受 cookies 但不回傳：拒絕　外送 方向。

點擊 完成。

19.5. Script 管控

Scripts 及其他類似 ActiveX 管控 及 Java applets，是被用來建立互動式網頁，可以被設計成有害的程式。舉例來說，ActiveX 元素可以獲取您的資料，它們可以從您的電腦讀取資料、刪除資訊、擷取密碼並在您上線時攔截訊息。您應該只接受您所信任網站的主動式內容。

BitDefender 讓您選擇去執行這些元件或者封鎖它們的執行。

透過 Script 管控 您可以指定哪個網站是您信任或者不信任。BitDefender 將會先徵求您的同意無論何時一個網站試著啟動一個 script 或其他主動式的內容：



Script 警示

您可以檢視資源的名稱。

點擊記住這個答案 選項並按下 確定 或取消 ，一個規則將被建立、套用並列於規則表格中。當相同網站試圖寄送您一個主動式的內容時，您將不再受到通知。

要設置Script管控，請在進階檢視中進入隱私權管控>Script。

Script 管控

您可以在表格中檢視目前已建立的規則清單。



重要

規則將依序它們的優先權由上而下排列，越高就越優先。拖曳這些規則以更改他們的優先權。

要刪除一個規則，只需點選規則並點擊 刪除鈕。 要更改這些規則參數，雙擊規則並在設置視窗中更改。

要手動增加規則，點擊 加入鈕並在視窗中設置規則參數。

19.5.1. 設置視窗

當您編輯或手動加入一個規則時，設置視窗將出現。

選擇位址與動作

您可以設置參數：

- 網域位址 - 在規則裡，輸入所應套用的網域。
- 動作 - 選擇規則所要執行的動作。

動作	描述
允許	在這個網域的 scripts 將會被執行。
拒絕	在這個網域的 scripts 將不會被執行。

點擊 完成。

20. 防火牆

防火牆保護您電腦免於未授權的內送或外送連線威脅。它就像您網路的警衛一樣 - 注意您的網際網路連線，並追蹤誰要允許網際網路、誰要阻擋存取。



註
如果您有寬頻或DSL連線，防火牆是必要的。

在隱匿模式下，您的電腦將會”隱藏”避免暴露於惡意軟體及駭客的威脅。防火牆模組有能力可以自動偵測並防範連接埠掃描 (一連串的封包傳送到電腦以找出”存取點”，這通常是駭客攻擊前的準備工作)。

20.1. 設定

要設置防火牆防護，請在進階檢視進入防火牆>設定。



防火牆設定

您可以查看BitDefender防火牆是否啟動。 如果您想更改防火牆狀態，請選取對應的方塊。



重要

防護您的系統抵抗網際網路的攻擊，請保持 防火牆 啟動。

有兩類的資訊：

- 網路設置概要. 您可以查看您的電烤名稱、IP位置與預設閘道。 如果您有一個以上的網路卡(代表您連結一個以上的網路)，您將看到每一個網路卡的IP位置與閘道設置。
- 統計數據. 您可以查看關於防火牆活動的統計：
  - 已傳送的位元組。

- 已接收的位元組。
- BitDefender已偵測並阻擋的連接埠掃描數量。 連接埠掃描時常被駭客來尋找您開啟的連接埠。
- 已丟棄的封包數量。
- 開啟的連接埠數量。
- 內收連結的數量。
- 外送連結的數量

要查看活動的連結和開啟的連接埠，請前往活動標籤。

您可以在頁面底端查看BitDefender關於接收和外送傳輸的統計。圖表顯示先前二分鐘的傳輸網路量。



註
即使防火牆停用，這個圖形仍會出現。

20.1.1. 設定預設活動

預設上，BitDefender自動允許所有白名單上的程式存取網路。 其他未在白名單上的程式，BitDefender將出現警告視窗提醒您是否進行此活動。 您指定的行動將隨時套用在應用程式需要網路存取時。

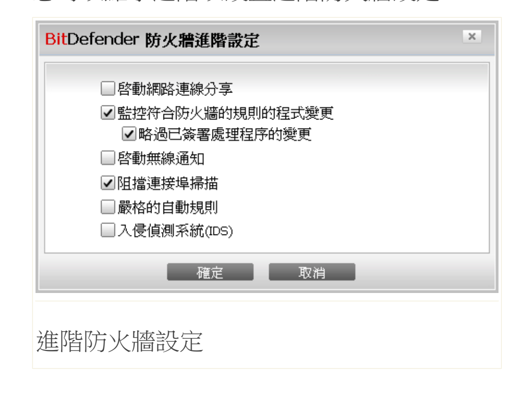
您可以拖曳滑桿設定當應用程式需要網路存取時，您要採取的行動。 可使用以下的預設行動：

預設行動	描述
允許全部	套用目前的規則，並且不需提示就允許所有與目前規則不符的傳輸企圖。 強烈不建議設定此種做法，但它也許對網路系統管理者或是遊戲玩家是有用的。
允許已知程式	套用目前的規則，並允許所有已加入白名單的程式外送連結企圖。BitDefender將詢問您其他的連結企圖。 白名單中的程式是世界通用常見的應用程式。包含常見的網路瀏覽器、多媒體播放器、交談和檔案共享的程式，以及伺服器用戶與作業系統的應用程式。

預設行動	描述
報告	套用目前的規則，並詢問您任何與現行規則不符的傳輸企圖。
全部拒絕	套用目前規則，並拒絕所有不符合目前規則的傳輸企圖。

20.1.2. 設置進階防火牆設定

您可以點擊進階以設置進階防火牆設定。



進階防火牆設定

以下的選項是可用的：

■啟動網際網路連線分享(ICS)支援 - 啟動網際網路連線分享(ICS)的支援。



註
這個選項不會自動啟動網際網路連線分享，只會在您從作業系統啟動這類型的連線時允許連線。

網際網路連線分享(ICS) 允許區域網路電腦透過您的電腦存取到網際網路。當您處於一個特別的網際網路連線(如：無線網路)時，您可以透過這種方式，分享網際網路的連線給區域網路內的其他電腦。

與本地區域網路的成員分享您的網際網路連接可能導致系統資源消耗較大、可能有一些風險，並且使用您網路連線的成員將開啟您的一些連接埠。



- 監控符合防火牆規則的程式檔案變更 - 檢查存取規則新增後，每一個試圖連接到網際網路的應用程式是否有變更。如果應用程式被變更，將出現警告提醒您選擇允許或阻檔應用程式存取網際網路。

  通常應用程式是由於更新造成變更，但也有可能是惡意程式為感染您的電腦和其他電腦造成。

  註
  建議您保持此選項啟動，並在存取規則建立之後，只允許變更你希望的應用程式。

  已標記的應用程式是被信任的，並且有高度安全性。 您可以檢查略過已標記的處理程序變更可以允許更改過的已標記應用程式連結至網路，不需警告您。

- 啟動無線網路提示 - 若您連線至無線網路，顯示關於特定網路事件資訊視窗(例如新電腦加入網路)。
- 阻擋連接埠掃描 - 偵測並阻擋連結埠掃描企圖。

  駭客常使用連結埠掃描來找尋您電腦開啟的連結埠。 若駭客找到可用的連接埠或安全弱點，將可能闖入您的電腦。

- 嚴格的自動規則 - 建立嚴格的規則。 如果這個選項啟動，當不同的處理程序開啟需要網路存取的應用程式時，BitDefender將提示您進行行動或是建立規則。
- 侵入偵測系統(IDS) - 對試圖存取網路的應用程式進行啟發式監控。

20.2. 網路

要設置防火牆設定，請在進階檢視進入防火牆>網路。



網路

網路設置目錄中的欄位提供您連結的網路詳盡資訊：

■網路卡 - 您的電腦使用連結至網路的網路卡。

■類型 - 網路卡的信任層級。 根據網路卡設置，BitDefender 將自動指定信任層級，或詢問您。

■隱匿 - 這台電腦是否能被其他電腦偵測到。

■一般 - 一般設定是否能套用至這個連線。

■位址 - 此網路卡的IP位置。

■閘道 - 您電腦連線至網路的IP位置。

20.2.1. 改變信任層級

BitDefender指定每一個網路卡信任層級。 信任層級顯示網路卡的可信任程度。

根據信任層級，網路卡將根據系統與BitDefender如何存取網路來建立特定的規則。

您可以在網路設置目錄中的類型欄位下查看網路卡的信任層級。 要更改信任層級，點擊類型欄位的箭頭並選擇。

安全層級	描述
完全信任	停用網路卡的防火牆。
本地信任	允許本地網路的所有傳輸。
安全	允許在本地網路分享資源。 這是本地(家庭或辦公室)網路的預設層級。
不安全	停止網路上的電腦連結至您的電腦。 此層級是公用網路(如果您收到一個IP位置是從網際網路服務提供者而來)的預設層級。
阻擋本地	在本地網路阻擋所有傳輸以及網路存取。 此層級是不安全(公開) 的無線網路預設層級。
阻擋	完全阻擋該網路卡的網路傳輸。

20.2.2. 設置隱匿模式

隱匿模式隱藏您的電腦，遠離惡意程式及駭客。 要設置隱匿模式，請點擊隱匿欄位上的箭頭▾，並選擇想要的選項。

隱匿選項	描述
開啟	隱藏模式已開啟。 您的電腦無法被本地網路及網際網路看到。
關閉	隱匿模式已關閉。 本地網路及網際網路都可以偵測到您的電腦。
遠端	您的電腦無法被網際網路使用者偵測到。 本地網路使用者仍能偵測到您的電腦。

20.2.3. 設置一般設定

如果網路卡IP位置更改，BitDefender 也將隨之更改信任層級。 如果您想維持相同的信任層級，請點擊 一般 欄位上的箭頭 ▾ 並選擇 是。

20.2.4. 網路區域

您可以在網路卡加入允許的或阻擋的電腦。

受信任的區域是您完全信任的電腦。 您的電腦間所有傳輸都被允許。 要與特定電腦在不安全的無線網路下分享資源，請加入電腦至允許電腦。

受阻擋區域是您不希望與您連結的電腦。

區域 - 顯示目前每個網路卡的網路區域的表。

要增加一個區域，請點擊 加入鈕。

BitDefender 增加區域

區域：

10.10.0.1 - core.dsd.ro
10.10.0.2 - dc.dsd.ro
10.10.0.3 - gwintern.dsd.ro
10.10.0.4 - vpn.dsd.ro
10.10.0.5
10.10.0.6
10.10.0.7 - hp5550.dsd.ro
10.10.0.8 - hp1022.dsd.ro
10.10.0.9
10.10.0.10
10.10.0.17

行動：
允許 拒絕

確定 取消

加入區域

步驟如下：

1. 選擇您想加入的電腦IP位置。
2. 選擇行動：
   - 允許 - 允許您電腦間的所有傳輸。

■拒絕 - 阻擋您電腦間的所有傳輸。

3. 點擊確定。

20.3. 規則

要管理應用程式存取網路的防火牆規則，請在進階檢視進入防火牆>規則。



防火牆規則

您可以查看防火牆規則建立的應用程式(處理程序)。　　　如果您想查看關於系統或BitDefender處理程序的規則，請取消選取隱藏系統規則方塊。

要查看特定應用程式的規則，請點擊該應用程式旁的+方塊。 您可以得知每一個規則的詳盡資訊，顯示在表欄：

■處理程序/網路卡類型 - 該處理程序與網路卡的規則套用類型。 自動建立規則以過濾透過任何網路卡的網路存取。 您可以手動建立或編輯規則以過濾應用程式透過特定網路卡的網路存取(例如，無線網路卡)。

■指令列 - 使用在Windows 指令介面開始處理程序的指令。(cmd).

■通訊協定 - 規則套用的IP通訊協定。 您可能看到下列其中之一：

通訊協定	描述
任何	包含所有IP通訊協定。
TCP	傳輸控制協議(TCP) - TCP保證資料的傳輸以及封包的傳輸次序。
UDP	用戶數據報協議(UDP) - UDP是以 IP 為基礎的運輸系統，有較強的表現。遊戲或是影音應用程式常使用 UDP 。
數字	表示其他的IP通訊協定。 您可以在 www.iana.org/assignments/protocol-numbers找到完整的IP通訊協定數字清單。

■網路事件 - 規則套用的網路事件。 下列事件可能被考量：

事件	描述
連結	連接導向的通訊協定使用(例如TCP)的標準訊息初步交換，以建立連結。 由於連結導向的通訊協定，兩台電腦的資料傳輸只在連結建立之後才發生。
傳輸	兩台電腦間的資料流量。
聆聽	應用程式監控網路等候建立連結或從同級的應用程式接收資訊的狀態。

■本地連接埠 - 您的電腦中規則套用的連接埠。

■遠端連接埠 - 遠端電腦中規則套用的連接埠。

■本地 - 規則是否僅套用在本地網路電腦。

■行動 - 在特定情況是否允許應用程式存取網路。

20.3.1. 自動地新增規則

當 防火牆 啟動時，每當要存取網際網路的連線時，BitDefender 將徵求您的同意：



防火牆警示

您可以檢視以下的訊息：哪些應用程式嘗試存取網際網路，透過什麼通訊協定、IP位址，及應用程式正在嘗試連接哪一個連接埠。

點擊允許以允許這個應用程式在特定的IP通訊協定和在所有連接埠的所有傳輸(內送和外送)。 如果您點擊阻擋，將拒絕應用程式透過特定的ip通訊協定存取網際網路。

將以您的答案建立規則，並且套用、陳列在表上。下一次此應用程式嘗試連結時，此規則將被自動套用。



重要

只允許您絕對信任的 IP 位址或網域進行內送的連線企圖。

20.3.2. 刪除規則

要刪除規則，選擇並點擊 移除規則鈕。 您可以一次選擇並刪除多個規則。

要刪除特定應用程式的所有規則，請從清單選擇應用程式並點擊 移除規則鈕。

20.3.3. 建立與更改規則

手動建立新的規則並更改現有規則，在設置視窗更改參數。

建立規則. 要手動建立規則，請依照下列步驟：

1. 點擊 加入規則鈕。 設置視窗將會出現。
2. 設置需要的主要與進階參數。
3. 點擊確定已加入新的規則。

修改規則. 要修改現存規則，請依照下列步驟：

1. 點擊 編輯規則鈕或雙擊規則。 設置視窗將會出現。
2. 設置需要的主要與進階參數。
3. 點擊確定 以儲存變更。

設置主要參數

設置視窗的主要標籤提供您設置主要的規則參數。



主要參數

您可以設置下列參數：

- 程式路徑. 點擊瀏覽並選擇要套用規則的應用程式。 如果您想要規則套用到全部的應用程式，選擇任何。
- 命令列. 如果您想要將規則只套用至指定的應用程式，您可以取消選取任何，並在Windows指令列頁面中輸入對應的指令。
- 通訊協定. 從選單選擇要套用規則的IP通訊協定。

- 如果您想要規則套用到全部的通訊協定，選擇任何。
- 如果您想套用規則至特定的通訊協定，請選擇其他。 一個新的編輯欄位將會開啟。 在編輯欄輸入您想過濾的通訊協定數字。



註

IP通訊協定數字是由Internet Assigned Numbers Authority (IANA)所訂定。 您可以在www.iana.org/assignments/protocol-numbers找到完整的IP通訊協定數字清單。

■事件. 根據所選的通訊協定，選擇規則套用的網路事件。 下列事件可能被考量：

事件	描述
連結	連接導向的通訊協定使用(例如TCP)的標準訊息初步交換，以建立連結。 由於連結導向的通訊協定，兩台電腦的資料傳輸只在連結建立之後才發生。
傳輸	兩台電腦間的資料流量。
聆聽	應用程式監控網路等候建立連結或從同級的應用程式接收資訊的狀態。

■安全層級. 選擇規則套用的信任層級。

■動作. 選擇下列可用行動的其中之一：

動作	描述
允許	允許指定的應用程式在指定的環境存取網際網路。
拒絕	拒絕指定的應用程式在指定的環境存取網際網路。

設置進階參數

設置視窗的進階標籤提供您設置進階的規則參數。



進階參數

您可以設置下列進階參數：

■方向．　從選單選擇規則套用的傳輸方向。

方向	描述
外送	這個規則只套用外送的傳輸。
內送	這個規則只套用內送的傳輸。
兩者皆是	這個規則套用到進出二個方向。

■IP版本．　從選單選擇規則套用的IP版本(IPv4，IPv6 或任何其他)。

■本地位置．　指定規則套用的本地IP位置與連接埠如下：

- 如果您有一章以上的網路卡，您可以取消選取任何方塊並輸入指定的IP位置。
- 如果您已經選擇TCP或UDP通訊協定，您能設定一個指定的連接埠、或0到65535之間的範圍。如果您想要規則套用到全部的通訊協定，選擇任何。

■遠端位址．　指定規則套用的遠端IP位置與連接埠如下：

- 要過濾您的電腦與另一台特定電腦的傳輸，請取消選取任何方塊並輸入其IP位置。
- 如果您已經選擇TCP或UDP通訊協定，您能設定一個指定的連接埠、或0到65535之間的範圍。如果您想要規則套用到全部的通訊協定，選擇任何。

■只套用此規則於直接連結的電腦。． 若您只想套用規則於本地傳輸企圖，選擇這個選項。

■檢查原始事件的主程序串． 只有在您已選擇嚴格的自動規 嚴格的規則代表當您的應用程式要求存取跟主程序不同的網路時，BitDefender會提醒您。

20.3.4. 進階規則管理

如果您需要管控進階防火牆規則，請點擊進階。 一個新的視窗將會開啟。



進階規則管理

您可以查看根據紀錄順序排序的防火牆規則。 此表欄提供每一個規則的詳盡資訊。



註

當產生一個連結企圖時(無論是內收或外送)，BitDefender 將套用首先符合連結的行動。 因此，規則的排序十分重要。



要刪除規則，選擇並點擊 刪除規則鈕。

要編輯一個規則，只需點選規則並點擊 編輯規則鈕或者雙擊它。

您可以更改規則的優先順序。在選擇的規則上，點擊 上移鈕增加優先順序或點擊 下移 按鈕減低其優先順序。 要將一個規則設為最高優先，點擊 移到最上方鈕。要將規則設為最低優先，點擊 移到最下方按鈕。

按下 關閉 關閉視窗。

20.4. 連線管控

要監控目前應用程式分類的網路活動(透過TCP和UDP)，請在進階檢視進入防火牆>活動。



連線管控

您能見到應用程式分類的所有傳輸、以及每個應用程式的連結與開啟的連接埠口、外送與內收的傳輸速度與資料傳送/接收到的全部數量統計。

如果您也想要查看閒置的處理程序，取消選取隱藏閒置處理程序方塊。

圖示的意義如下：

■ 顯示您電腦的一個開啟的連結。

■ 顯示您電腦的一個開啟的連接埠。

視窗即時地呈現目前的網路活動。當連接或連接埠被關閉，您能見到對應的統計資料漸漸減少，最後消失。 同樣的，產生傳輸或開啟連接埠的應用程式若被您關閉，對應的統計資料也會漸漸減少，最後消失。

要檢視關於防火牆模組處理(如啟動/停用防火牆、阻擋傳輸、更改設定)或模組偵測到的行動(如掃描連接埠、阻擋連結企圖或規則相關的傳輸)的完整清單，請點擊顯示日誌檢視BitDefender 防火牆日誌。 這個檔案位於目前Windows使用者的Commom Files資料夾中，路徑為：...BitDefender\BitDefender Firewall\bdfirewall.txt。

如果您想要讓日誌包含更多資訊，請選擇增加日誌敘述。

21. 加密

BitDefender提供加密功能，防護您的機密文件和您透過Yahoo即時通與MSN Messenger的即時交談對話。

21.1. 即時通訊加密

BitDefender加密所有您的即時交談訊息，預設規定：

- 您的交談對象已安裝了支援即時通訊加密的BitDefender版本，並且即時通訊加密在您的即時通訊程式上已經啟動。
- 您和您的交談對象使用Yahoo即時通或是Windows Live (MSN) Messenger交談。



重要

若您的交談對象使用，如Meebo、或其他支援Yahoo即時通與Windows Live (MSN) Messenger的網頁型的交談程式，BitDefender將無法加密對話。

要設置即時通訊加密，請在進階檢視中進入加密>即時通訊加密。



註

您可以從交談視窗中使用BitDefender工具列，輕易的設置即時通訊加密。 請參閱"整合進入即時通訊" (p. 51)，以獲得更多資訊。



即時通訊加密

預設即時通訊加密同時在Yahoo 即時通和Windows Live (MSN) Messenger 上啟動。您可以選擇在特定的或所有的即時通訊程式上停用即時通訊加密。

顯示兩份表格：

■加密例外－停用加密的使用者帳號和對應的即時通訊程式。 要從清單上移除聯絡人，選取並點擊⊟ 移除鈕。

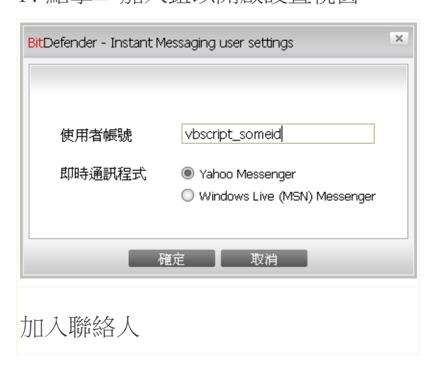
■目前的連線 －目前使用中的即時通訊軟體及對應的聯絡人清單，以及它們是否啟動加密。 連線有以下幾個可能沒有被加密：

- 您在對應的連線上已停用加密。
- 您的連絡人沒有安裝支援即時通訊加密的BitDefender 版本。

21.1.1. 對特定的使用者停用加密

要對特定的使用者停用加密，請依照以下步驟：

1. 點擊 加入鈕以開啟設置視窗。



加入聯絡人

2. 在編輯欄位輸入聯絡人的使用者名稱。
3. 選取聯絡人對應的即時通訊程式。
4. 點擊確定。

21.2. 檔案保險箱

BitDefender 檔案保險箱讓您能夠建立一個加密、有密碼保護的磁碟在您的電腦上，並能夠安全的儲存您私密及敏感的文件。 儲存在保險箱中的資料只能經由知道密碼的使用者存取。

密碼讓您能夠開啟、儲存資料以及關閉保險箱並維持安全性。 當保險箱開啟時，您可以加入新檔案、存取原有的檔案或變更它們。

保險箱檔案以.bvd作為副檔名儲存在您的電腦中。 雖然保險箱檔案可以在其他的作業系統(如Linux)存取，但是保險箱內儲存的訊息已經過加密無法使用。

要管理您電腦上的檔案保險箱，請在進階檢視選擇加密>檔案保險箱。

檔案保險箱

要停用檔案保險箱，清除檔案保險箱已啟動核取方塊並點擊是以確認操作。 如果您停用檔案保險箱，所有的檔案保險箱都將上鎖，而您再也無法存取內容檔案。

上方的表格顯示您電腦上的檔案保險箱。 您可以檢視保險箱名稱、狀態(開啟/上鎖)、磁碟代號以及完整路徑。 下方的表格顯示選取的保險箱內容。

21.2.1. 建立保險箱

要建立新的保險箱，使用以下任何一種方法：

■點擊 建立保險箱。

■在保險箱表格中點擊右鍵並選取建立。

■在您的桌面或電腦中的資料夾上點擊右鍵，指向BitDefender檔案保險箱然後選取建立。

一個新的視窗將會開啟。

建立檔案保險箱

步驟如下：

1. 指定保險箱檔案的位置和名稱。
   - 點擊瀏覽，選取保險箱檔案的位置然後指定您想要的名稱。
   - 輸入保險箱檔案的完整路徑。
2. 從選單選擇磁碟代號。 當您開啟了保險箱，我的電腦中將會以您指定的磁碟代號開啟一個虛擬磁碟。
3. 在 密碼 欄位輸入保險箱密碼。 任何想要開啟保險箱和存取檔案的使用者都必須輸入密碼。
4. 選取格式化磁碟以格式化指定給保險箱的虛擬磁碟。
5. 如果您想要變更保險箱預設大小(50 MB)，在保險箱大小欄位輸入想要的數值。
6. 點擊建立如果您只想要在選取的位置建立保險箱。 要建立並顯示保險箱為一個在我的電腦中的虛擬磁碟，點擊建立&開啟。

21.2.2. 開啟保險箱

要存取並使用保險箱內的檔案，您必須開啟保險箱。 當您開啟了保險箱，我的電腦中將會出現一個虛擬磁碟。 保險箱磁碟將會被指派您所指定的磁碟代號。

要開啟保險箱，使用以下任何一種方法：

■從表格中選取保險箱並點擊 開啟保險箱。

■在表格中右鍵點擊保險箱並選取開啟。

■右鍵點擊您電腦中的保險箱檔案，指向BitDefender 檔案保險箱然後選取開啟。

一個新的視窗將會開啟。

BitDefender 2009 - 開啓保險箱檔案

保險箱檔案在磁碟上的完整路徑

D:\Documents and Settings\Administrator\my documents\miki.bvd

磁碟代號：J: 密碼

開啓 取消

開啟檔案保險箱

步驟如下：

1. 從選單選擇磁碟代號。

2. 在 密碼 欄位輸入保險箱密碼。

3. 點擊開啟。

21.2.3. 將保險箱上鎖

當您結束了檔案保險箱內的工作，您必須將它上鎖以確保資料安全。

要將保險箱上鎖，使用以下任何一種方法：

■從表格中選取保險箱並點擊 將保險箱上鎖。

■在表格中右鍵點擊保險箱並選取將保險箱上鎖。

■右鍵點擊您電腦中的保險箱檔案，指向BitDefender 檔案保險箱然後選取上鎖。

■在我的電腦中對應的虛擬磁碟上點擊右鍵，指向BitDefender檔案保險箱然後選取上鎖。

21.2.4. 變更保險箱密碼

要變更保險箱密碼，使用以下任何一種方法：

- 從表格中選取保險箱並點擊 變更密碼。
- 在表格中右鍵點擊保險箱並選取變更密碼。
- 右鍵點擊您電腦中的保險箱檔案，指向BitDefender 檔案保險箱然後選取變更保險箱密碼。

一個新的視窗將會開啟。



變更保險箱密碼

步驟如下：

1. 在 舊密碼欄位輸入原有的密碼。
2. 在新密碼欄位輸入新密碼，在確認新密碼欄位重新輸入密碼。



註

密碼長度至少要八個字元。 使用大小寫混用、數字或特殊符號（例如#、$或@），以加強密碼。

3. 點擊確定儲存密碼。

21.2.5. 加入檔案至保險箱

要加入檔案至保險箱，請依照以下步驟：

1. 點擊 加入檔案。 一個新的視窗將會開啟。
2. 選取要加入保險箱的檔案/資料夾。
3. 點擊 確定將選定的目標複製至保險箱。



註
您無法將系統檔案或應用程式加入保險箱。

21.2.6. 從保險箱移除檔案

要從保險箱移除檔案，請依照以下步驟：:

1. 從表格中選取您要移除檔案的保險箱。
2. 從保險箱內容表格中選取您要的移除檔案。
3. 點擊× 移除檔案。



註
如果檔案保險箱開啟，您可以直接從虛擬磁碟中移除檔案。

22. 弱點檢查

定期更新您所使用的作業系統以及重要應用程式，是保護您的電腦免於惡意程式威脅的重要步驟。　　此外，為了防止未經認可的來源存取您的電腦，您必須為您的每個 Windows 帳號設置安全的密碼。

BitDefender 會定期的檢查您的系統弱點並通知您存在的事件。

22.1. 狀態

要設置自動系統弱點檢查或執行系統弱點檢查，請在進階檢視選擇系統弱點>狀態。



系統弱點狀態

這表格顯示前一次弱點檢查的結果以及狀態。 您能檢視每個用來修復弱點的動作，如果有的話。 若動作為無，則該事件不會成為系統弱點。





重要

要自動通知您的系統或應用程式弱點，請保持 自動系統弱點檢查 啟動。

22.1.1. 正在修復系統弱點

要修復特定的弱點，點兩下該事件並進行以下動作:

- 若有可用的Windows更新，點擊安裝所有系統更新以安裝所有可用的更新。
- 若應用程式未更新，請使用首頁連結以更新到最新版本。
- 若Windows帳戶的密碼有危險性，強制使用者於下次登入時變更密碼，或自行變更。

您可點擊立刻檢查並依照精靈的步驟進行弱點修復。

步驟 1/6 - 選擇要檢查的系統弱點



系統弱點

點擊下一步以檢查系統已選的弱點。

步驟 2/6 – 系統弱點檢查



系統弱點檢查

等待BitDefender 完成系統弱點檢查。

步驟 3/6 – 更改不安全的密碼



使用者密碼

您可以檢視您電腦中的Windows使用者帳戶清單，以及他們的密碼防護層級。點擊修復以更改不安全的密碼。 一個新的視窗將會開啟。

BitDefender

Choose method to fix:

Force user to change password at next login

Change user password

Type password:

Confirm password:

OK Close

更改密碼

選擇修復此事件的方法：

- 強迫使用者在下次登入時更改密碼. BitDefender將提示使用者在下次登入Windows時更改密碼。
- 更改使用者密碼. 您必須在文字框輸入新的密碼。



註
使用大小寫混用、數字或特殊符號 (例如#、$或@)，以加強密碼。

點擊確定儲存密碼。

點擊 下一步。

步驟 4/6 – 更新應用程式



應用程式

您可以查看BitDefender檢查的的應用程式清單及他們的更新狀態。 若應用程式未更新，請點擊連結以更新到最新版本。

點擊 下一步。

步驟 5/6 - 更新Windows



Windows更新

您可以查看您尚未安裝的Windows更新清單。 點擊安裝所有系統更新以安裝所有可用的更新。

點擊 下一步。

步驟 6/6 - 檢視結果



結果

點擊關閉。

22.2. 設定

要設置自動系統弱點檢查，請在進階檢視選擇系統弱點>狀態



自動系統弱點檢查設定

選取對應的核取方塊以指定您想要定期檢查的系統弱點。

■重大Windows更新

■定期Windows更新

■在 危險的密碼

■應用程式更新



註
如果您沒有選取系統弱點對應的核取方塊，BitDefender 將不再通知您相關的事件。

23. 遊戲/筆電模式

遊戲/筆電模組允許您設置特別的BitDefender 運行模式。

- 遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。
- 筆電模式能夠在您的筆電使用電池為電源時停用排定要執行的任務，以節省電池電力。

23.1. 遊戲模式

遊戲模式能夠暫時地變更防護設定，將系統運行的影響減至最低。 當您啟動遊戲模式，下列設定將會被套用：

- BitDefender警示及彈出示提示已全部停用。
- BitDefender 即時防護層級設定在 寬鬆e。
- BitDefender 防火牆是設定為 全部允許。 這代表所有的連結都將自動允許，不論它們使用什麼連接埠和通訊協定。
- 預設為不執行更新。



註
要變更設定，請至更新>設定 並取消選取 開啟遊戲模式時不要更新。

- 預設為停用排定的掃描任務。

預設BitDefender 會在您所設定的遊戲或全螢幕應用程式啟動時自動開啟遊戲模式。 您可以手動進入遊戲模式，鍵入熱鍵Ctrl+Alt+Shift+G。 強烈建議您離開遊戲後關閉遊戲模式，您可以使用相同的熱鍵Ctrl+Alt+Shift+G以離開



註
當遊戲模式啟動時，您可以看見英文字母G顯示在 BitDefender圖示上。

要設置遊戲模式，請在進階檢視選擇遊戲 / 筆電 Mode;遊戲模式。



遊戲模式

您可以在此頁面的最上方檢視遊戲模式狀態。 您可以點擊進入遊戲模式或離開遊戲模式以變更目前狀態。

23.1.1. 設置自動遊戲模式

自動遊戲模式允許BitDefender 在偵測到執行遊戲時，自動進入遊戲模式。 您可以設置下列選項：

■使用BitDefender提供的遊戲清單－以允許BitDefender 在偵測到正在執行清單上的遊戲時，自動進入遊戲模式。 要檢視清單，點擊管理遊戲然後點擊檢視已允許的遊戲。

■當切換至全螢幕時進入遊戲模式－當您使用的應用程式進入全螢幕時，自動切換至遊戲模式。

- 加入應用程式至遊戲清單？－在離開使用全螢幕的應用程式時，提醒是否加入遊戲清單。 如果將一個新的應用程式加入遊戲清單，下次您執行這個程式時將會自動進入遊戲模式。



註
如果您不想要BitDefender自動進入遊戲模式，請取消選取自動遊戲模式核取方塊。

23.1.2. 管理遊戲清單

在您執行遊戲清單上的應用程式時，BitDefender 將自動進入遊戲模式。 要檢視並管理遊戲清單，點擊管理遊戲。 一個新的視窗將會開啟。



遊戲清單

當這些時候新的應用程式將自動加入清單：

- 您開啟了一個BitDefender已知的遊戲。 要檢視清單，點擊檢視已允許的遊戲。
- 在離開使用全螢幕的應用程式時，您在提醒視窗將它加入了遊戲清單。

如果您想要針對某個應用程式停用自動遊戲模式，請取消選取對應的核取方塊。 您應該針對某些時常使用全螢幕的應用程式停用自動遊戲模式，如瀏覽器或影音播放器。

要管理遊戲清單，您可以使用表格上方的按鈕。

- 加入以加入新的程式至遊戲清單。
- 移除 — 從遊戲清單中移除應用程式。
- 編輯 - 編輯已存在的遊戲清單。

加入或編輯遊戲

如果您加入或編輯了遊戲清單，將會出現以下視窗：



加入遊戲

點擊瀏覽以選取應用程式或在編輯欄位中輸入應用程式的完整路徑。

如果您不想在選定的應用程式執行時自動進入遊戲模式，點擊停用。

點擊確定以新增程式至遊戲清單。

23.1.3. 設置遊戲模式設定

要設置停止哪些排定的任務，選取這些選項：

- 掃描任務 — 避免在遊戲模式時啟動排定的掃描任務。 您可以選取下列選項的其中之一：

選項	描述
跳過任務	不要執行排定的任務。
延緩任務	在您離開遊戲模式後立刻執行排定的任務。

要在遊戲模式中自動停用防火牆，請依照以下步驟：

1. 點擊進階設定。 一個新的視窗將會開啟。
2. 選取不要使用防火牆核取方塊。
3. 點擊確定 以儲存變更。

23.1.4. 變更遊戲模式熱鍵

您可以手動進入遊戲模式，鍵入熱鍵Ctrl+Alt+Shift+G。 如您想更改快速鍵，請按照以下步驟：

1. 點擊進階設定。 一個新的視窗將會開啟。



進階設定

2. 在使用熱鍵選項，設定您要的熱鍵：
   - 您可以按下：Ctrl鍵(Ctrl)、Shift鍵(Shift)、Alt鍵(Alt)以選擇使用它們當做熱鍵。
   - 在編輯欄鍵入字母以對應熱鍵。

   舉例而言，如果您想要用Ctrl+Alt+D當作熱鍵，您必須按下Ctrl與Alt並且輸入D。
3. 點擊確定 以儲存變更。



註
取消使用熱鍵旁的核取標記將停用熱鍵。



23.2. 筆電模式

筆電模式特別為筆電的使用者設計，將可以在您使用電池為電源時，對筆電的電力消費影響達到最低。

在筆電模式中，排定的任務預設為不執行。

BitDefender 偵測到您的筆電使用電池為電源時，將自動進入筆電模式。 而BitDefender 在偵測到您不再使用電池為電源時，將自動離開筆電模式。

要設置筆電模式，請在進階檢視選擇遊戲>筆電模式。



筆電模式

您可以檢視筆電模式是否啟動。 當使用筆電模式時，BitDefender 會套用使用電池時的設定。

23.2.1. 設置筆電模式設定

要設置停止哪些排定的任務，選取這些選項：

■掃描任務— 避免在筆電模式時啟動排定的掃描任務。 您可以選取下列選項的其中之一：

選項	描述
跳過任務	不要執行排定的任務。
延緩任務	在您離開筆電模式後立刻執行排定的任務。



24. 網路

網路模組提供您管理每一台家庭電腦中安裝的BitDefender。



網路區域

要管理您家庭電腦安裝的BitDefender，請您依照下列步驟：

1. 在您的電腦加入BitDefender家庭網路。 加入網路，為家庭網路管理設置一個管理者密碼。
2. 使用您想管理與加入網路的電腦，並設定密碼。
3. 回到您的電腦，並新增這些您想管理的電腦。

24.1. 加入BitDefender 網路

要加入BitDefender 家庭網路，請依照下列步驟：

1. 點擊加入/建立網路。 將提示您設置家庭管理密碼。



設置密碼

2. 在兩個文字框中輸入相同密碼。
3. 點擊確定。

您可以在網路地圖上看到電腦名稱。

24.2. 加入電腦至BitDefender 網路

加入電腦至BitDefender 網路前，您必須先在每一台電腦設置BitDefender家庭管理密碼。

要加入電腦至BitDefender 網路，請依照下列步驟：

1. 點擊管理網路。 將提示您輸入本地家庭管理密碼。

BitDefender

您必須輸入家庭管理的密碼。

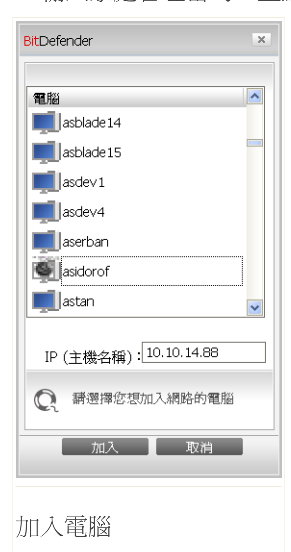
密碼: •••••••••••••

不要再顯示此訊息。

確定 取消

輸入密碼

2. 輸入家庭管理密碼，並點擊確定。 一個新的視窗將會開啟。



加入電腦

您可以檢視網路中的電腦清單。 小圖示的意義如下：

顯示一台線上電腦，但未安裝BitDefender。

顯示一台線上電腦，已安裝BitDefender。

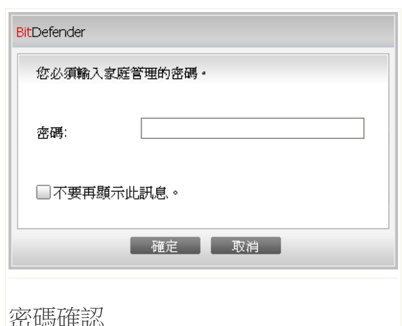
■  顯示一台離線電腦，已安裝BitDefender。

3. 您可以選擇以下動作：

■從清單中選擇要加入的電腦名稱。

■在對應欄位輸入要加入的電腦IP位置或電腦名稱。

4. 點擊加入。 將提示您輸入電腦的家庭管理密碼。



密碼確認

5. 輸入該電腦的家庭管理密碼。

6. 點擊確定。 若密碼輸入正確，該電腦將出現在網路地圖上。

註
您最多可以加入五台電腦至網路地圖。

24.3. 管理BitDefender網路

只要您成功建立一個BitDefender家庭網路，您就可以管理所有電腦中的BitDefender。



網路區域

移動游標至網路地圖上的電腦，您可以查看該電腦的資訊概要(名稱、IP位置、系統安全事件數量、BitDefender註冊狀態)。

在網路地圖上的電腦名稱點擊右鍵，您可以查看所有能在遠端電腦上執行的管理任務。

■註冊這台電腦

■設置設定密碼

■執行掃描任務

■在這台電腦上修復事件

■檢視此電腦歷史

■立即於此電腦執行更新

■套用至設定檔



■在此電腦執行調整任務

■設定此電腦為此網路的更新伺服器

在執行特定電腦的任務以前，將提示您輸入本地家庭管理密碼。



輸入密碼

輸入家庭管理密碼，並點擊確定。



註

若您要執行多個任務，您可以選擇這段期間不要再顯示這個訊息。 這樣，這段期間將不會再提示您輸入密碼。

25. 更新

每天都有新的惡意程式被發現及識別，所以保持最新的BitDefender病毒特徵碼非常重要。

如果您是透過寬頻或 ADSL 連線到網際網路，BitDefender 會特別注意更新。當您啟動您的電腦後，它將每 小時 確認更新。

自動更新設定。

更新程序正在進行中，代表原有的檔案正在被更新的檔案取代。在更新的同時，產品也不會有弱點。

更新會利用以下幾種方式：

■病毒防護引擎更新 —當新的威脅出現，病毒的特徵碼必須被更新以及時掃除具有特徵碼的檔案。這個更新的型態是我們熟知的病毒定義更新。

■反垃圾郵件引擎更新 — 新的規則將會被加入到啟發式和URL過濾器中，新的圖像會被加入到圖像過濾器。這將會增加您的反垃圾郵件引擎的效能 反垃圾郵件引擎更新。

■反間諜程式引擎更新 — 新的間諜程式特徵碼將會被加入到資料庫。這個更新的型態是我們熟知的 反間諜程式更新。

■軟體更新 — 當一個新的軟體版本被發行時，新的功能的掃描技術都用以提升軟體的效能，這個更新的型態是我們熟知的 軟體更新。

25.1. 自動更新

要檢視更新的相關資訊並執行自動更新，請在進階檢視選擇更新>更新。



自動更新

您可以在此檢視最近一次的更新是何時進行的、更新時是否成功。防毒引擎的版本資訊以及所有的特徵碼數量也會在此顯示。

如果您在更新的過程開啟此頁面，您將能夠檢視狀況。



重要

為了防護您的系統以抵抗最新的病毒威脅，請保持 自動更新 啟動。

您可以透過點擊顯示病毒清單以取得BitDefender的惡意程式特徵碼。一個HTML檔案將會被建立並包含所有可用的特徵碼在您的瀏覽器上。您可以透過資料庫搜尋特定的惡意程式特徵碼，或點擊BitDefender病毒清單到線上BitDefender特徵碼資料庫。

25.1.1. 正在要求更新

點擊Update Now以隨時在您想要的時候進行自動更新。這個更新的型態是我們熟知的使用者要求的更新。

這個 更新 模組將連線到 BitDefender 更新伺服器並且確認是否有更新可用。如果偵測到一個更新，將依據 手動更新設定 頁面的設定，您將被詢問是否要執行更新或者自動地安裝更新。



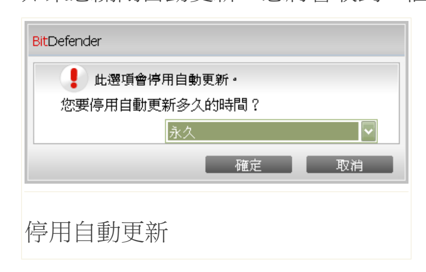
重要
當您完成更新時，可能需要將電腦重新啟動。我們建議盡可能重新開機。



註
如果您是利用撥接方式連線到網際網路，建議您定期地更新 BitDefender 以獲得最好的防護效果。

25.1.2. 停用自動更新

如果您關閉自動更新，您將會收到一個警告視窗。



停用自動更新

您可以從視窗選擇您要停用自動更新的時間長度。您可以選擇：5分鐘、15分鐘、30分鐘、一個小時、永久停用、或是直到下次系統重新開機。



警告
這將會是個重大安全事件，我們建議您盡可能減少停用自動防護的時間。如果BitDefender無法正常地執行更新，它將無法防護您的電腦抵抗最新的威脅。

25.2. 更新設定

可以從本地網路、或直接連線到網際網路或透過 Proxy 伺服器進行更新。 預設上，BitDefender能夠每小時檢查是否有新的可用更新並且能夠自動下載安裝到您的電腦。

要設置更新設定與管理proxy，請在進階檢視選擇更新>設定。



更新設定

在更新設定的視窗包含四個類型的選項 (更新位置設定、自動更新設定、手動更新設定 及 進階設定) 以可展開的選單方式呈現。

25.2.1. 更新位置設定

設定更新位置設定的位置 (登錄碼、Cookie)。這個設定透過更新位置設定目錄來進行。





註
設置這些設定，只有當如果您連接到地方性地儲存 BitDefender 惡意軟體驗證的一個本地區域網路，或者如果您經過一個proxy伺服器(Proxy)對網際網路連接。

為了更穩定及更快速地更新，您可以設置二個更新位置：一個是 主要更新位置，另一個是 次要更新位置。這兩個預設都是 http://upgrade.bitdefender.com。

要修改更新位置，在對應的URL欄位提供鏡像位置的URL。

註
我們推薦您設置主要更新位置為您身處的地區的鏡像，讓其他更新位置保持不變，以防萬一連不到本地的鏡像。

通常，公司會使用proxy伺服器連接網際網路，把使用proxy 打勾，並點擊管理proxy設置proxy設定。 更多資訊，請參閱"管理Proxy" (p. 264)

25.2.2. 設置自動更新

要設置BitDefender的自動更新程序，使用自動更新設定裡的選項。

您可以在時間間隔的欄位設定一段時間。預設上，更新時間間隔為一小時。

要指定自動更新如何執行，請選擇下列項目：

■隱匿更新 — BitDefender 自動地下載及執行更新。
■在下載更新前提示 — 每次當有更新可用時，在下載前先詢問您。
■在安裝更新前提示 — 每一次有下載更新時，在安裝前先詢問您。

25.2.3. 設置手動更新

要調整BitDefender的手動更新程序，選取手動更新設定裡的選項：

■隱匿更新 — 手動更新將自動地執行不會顯示使用介面。
■在下載更新前提示 — 每次當有更新可用時，在下載前先詢問您。

25.2.4. 設置進階設定

要避免BitDefender更新程序影響您的作業，請設置在進階設定目錄裡的選項：

- 等待重新開機以取代提示 — 如果一個更新要求重新開機時，軟體將仍以舊的檔案繼續運作，直到系統被重新開機。使用者將不會被提示重新開機，因此 BitDefender 更新程序將不會妨礙使用者的工作。
- 掃描中不要執行更新 — 如果正在執行掃描程序，BitDefender 將不會進行更新。這樣 BitDefender 更新程序將不會影響掃描工作。


註
當掃描正在進行時，如果 BitDefender 執行更新，則掃描程序將會被終止。

- 如果開啟遊戲模式，請勿更新 — 如果BitDefender遊戲模式設為開啟，則不會執行更新。 如此，您便能夠將產品對遊戲的影響最小化。

25.2.5. 管理Proxy

若您的公司使用proxy伺服器上網，您一定要設置proxy設定使BitDefender可以自己更新。否則，它會使用裝了產品的管理者proxy設定


註
Proxy設定只能被有管理權限的使用者調整。

要管理員proxy設定，點擊 管理proxy 。 Proxy管理員將會出現。

Proxy設定

管理者proxy設定(偵測於安裝時間)

位址： 連接 使用者名稱：

密碼：

目前使用者的proxy設定(從預設的瀏覽器)

位址： 連接 使用者名稱：

密碼：

指定您自訂的proxy設定

位址： 連接 使用者名稱：

密碼：

您可以在這裡更改管理者proxy設定。

確定 取消

Proxy管理員

Proxy設定有三組類別：

- ■管理者proxy設定(偵測於安裝時間) － 在安裝時偵測管理者帳號內的proxy設定，只有當您登入到該帳號時才能設置proxy。如果proxy伺服器需要一個使用者名稱和一個密碼，您一定要在對應的欄位中填上。
- ■目前使用者的proxy設定(從預設的瀏覽器)在目前使用者的預設瀏覽器中導出。如果proxy伺服器需要一個使用者名稱和一個密碼，您一定要在對應的欄位中填上。



註

支援的瀏覽器有Internet Explorer, Mozilla Firefox 和 Opera。若您預設使用其他的瀏覽器，BitDefender就不能夠讀取目前使用者設定。

- ■您自訂的proxy設定 — 當您以系統管理者登入時，您可以調整的proxy設定。

以下的選項是必須被指定的：

- 位址 — 輸入proxy伺服器的IP。
- 連接埠 — 輸入BitDefender 要使用連線到 Proxy 伺服器的連接埠。
- 使用者名稱 — 輸入 Proxy伺服器可識別的使用者名稱。



- 密碼 — 輸入先前指定使用者的有效密碼。

當嘗試連接到網路，每一組的proxy伺器設定都會去試，直至BitDefender連上。

首先，您自行設置的proxy設定會先連上網。若連不到，就會嘗試用在安裝時所讀取到的proxy設定來試。最後，如果都不行，就會用目前使用者預設瀏覽器的proxy來上網。

點擊 確定以儲存變更並關閉視窗。

點擊 套用－儲存變更或點擊 預設 載入預設值。

26. 註冊

要取得您的BitDefender完整資訊及註冊狀態，請在進階檢視選擇註冊。



註冊

這個頁面顯示：

■產品資訊：BitDefender的產品版本。

■註冊資訊：用來登入您的BitDefender帳號的電子郵件地址，目前的授權序號，以及還有幾天序號將會到期。

26.1. 註冊 BitDefender 網路安全2009

點擊立刻註冊以開啟產品註冊視窗。



註冊

您可以檢視BitDefender 註冊狀態，現在使用的授權序號，以及授權序號將在幾天內到期。

註冊 BitDefneder 網路安全 2009：

1. 選取 我想要以新的序號註冊產品。
2. 在編輯欄位中輸入授權序號。



註

您可以在這些地方找到授權序號：

■光碟標籤。
■產品註冊卡。
■線上購買的電子郵件。

如果您沒有BitDefender的授權序號，您可以連線至BitDefender 線上商店購買授權序號。

點擊 完成。

26.2. 建立一個 BitDefender 帳號

建立一個 BitDefender 帳號是註冊程序的重要步驟。 透過BitDefender帳號，您可以享有免費的更新服務、專業技術支援及特別的續購優惠。 如果您遺失了BitDefender授權序號，您可以透過http://myaccount.bitdefender.com並登入您的帳號以重新取得您的授權序號。



重要

您必須在安裝BitDefender15天內建立一個帳號(試用期將會被延長至30天)。 否則，BitDefender將不再繼續更新。

如果您還沒有建立BitDefender帳號，點擊建立一個帳號以開啟帳號註冊視窗。。



建立帳號



如果您不想建立 BitDefender 帳號，選取 跳過註冊並點擊完成。 否則，根據您目前的狀況選擇：

- "我沒有BitDefender 帳號" (p. 270)
- "我已經擁有BitDefender 帳號。" (p. 270)

我沒有BitDefender 帳號

選擇 建立新的 BitDefender 帳號 及提供所需的資料。 您在這裡所提供的資料將會被保密。

- E-mail address — 輸入您的電子郵件信箱。
- 密碼 — 為您的BitDefender帳號輸入一組密碼。 密碼長度至少要六個字元。
- 重複鍵入密碼 — 重新輸入先前的密碼。
- 名 — 輸入您的名字。
- 姓 — 輸入您的姓氏。
- "國家 —選擇您所在的國家。



註
在http://myaccount.bitdefender.com使用您提供的電子郵件地址和密碼來登入您的帳戶。

要成功建立一個帳號，您必須啟動您的電子郵件。確認您的電子郵件地址並依循 BitDefender 註冊服務所寄給您的電子郵件中的指示完成。

您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。選取一個選項：

- 傳送給我所有BitDefender的訊息
- 只傳送給我最重要的訊息
- 不要傳送任何訊息

點擊 完成。

我已經擁有BitDefender 帳號。

BitDefender 將會自動發現您先前電腦上登記的 BitDefender 帳號。 在這個情況下，請提供您的密碼。

如果您已經有一個帳戶,但是 BitDefender 並沒有偵測到，請選取登入到現有的 BitDefender 帳號並輸入您的電子郵件地址及密碼。

如果您忘記您的密碼，點擊 忘記您的密碼？ 並依循指示操作。

您可以在BitDefender帳號所登記的電子郵件信箱，收到特別的續購優惠的相關訊息。選取一個選項：

- 傳送給我所有BitDefender的訊息
- 只傳送給我最重要的訊息
- 不要傳送任何訊息

點擊 完成。

取得協助

27. 支援

作為一個具有價值的提供者，BitDefender 努力提供客戶一個快速且精確技術支援。支援部門（您可以透過以下提供的電子郵件地址與他們聯絡）不停地保持對抗最新的威脅。在這裡所有您提出的問題都會被及時地回覆。

BitDefender 專心致力減少客戶的時間及金錢，在一個合理的價格上提供最好的產品給客戶。此外，我們相信一個成功的事業是建購在良好的溝通及承諾提供卓越的客戶服務。

您可以在任何時間提出支援需求，利用以下的電子郵件帳號 support@bitdefender.com 為了迅速地回覆，請在您的郵件裡盡可能地詳述您的 BitDefender 版本、您的作業系統及您遇到的問題。

27.1. BitDefender 知識庫

BitDefender 知識庫是一個關於 BitDefender 產品的線上資訊庫。它利用很簡單易於存取的格式、由 BitDefender 支援及研發團隊提供不間斷的技術支援及錯誤修正、關於病毒預防的一般主題、詳細解釋 BitDefender 解決方案及其他更多的主題。

BitDefender 知識庫是公開並可自由地搜尋。它廣泛的資料包含提供買了BitDefender 的消費者所需技術上的知識。所有有效的資料請求或臭蟲報告都是來自BitDefender 的客戶。通常他們都能從BitDefender 知識庫，如 bugfix 報告、工作區、圖表 或者資訊的文章提供額外的支援。

BitDefender 知識庫可以在任何時間進行存取 http://kb.bitdefender.com。

27.2. 要求幫助

27.2.1. 前往網路自助服務

有問題？我們的安全專家會24/7存取電話、電子郵件在不用再付附加費的下幫助您。

請依照下列連結：

英語

http://www.bitdefender.com/site/KnowledgeBase/

德語

http://www.bitdefender.com/de/KnowledgeBase/

法語

http://www.bitdefender.com/fr/KnowledgeBase/

羅馬尼亞語

http://www.bitdefender.com/ro/KnowledgeBase/

西班牙

http://www.bitdefender.com/es/KnowledgeBase/

27.2.2. 開一張支援票

若您想開啟一張支援票並經由電子郵件接收支援。請選擇下列任一個連結：

英文網站：http://www.bitdefender.com/site/Main/contact/1/
德文網站：http://www.bitdefender.de/site/Main/contact/1/
法文網站：http://www.bitdefender.fr/site/Main/contact/1/
羅馬尼亞網站：http://www.bitdefender.ro/site/Main/contact/1/
西文網站：http://www.bitdefender.es/site/Main/contact/1/

27.3. 聯絡資訊

有效率的溝通是成功事業的關鍵。在過去十年中，BITDEFENDER已經建立一個無懈可擊的信譽，歷經不斷地努力溝通，超越客戶及夥伴的期望。如果您有任何問題，都希望不吝與我們聯絡。

27.3.1. 網站位址

業務部門：sales@bitdefender.com
技術支援部門：support@bitdefender.com
檔案相關問題：documentation@bitdefender.com
夥伴計劃：partners@bitdefender.com

市場行銷 marketing@bitdefender.com
媒體相關：pr@bitdefender.com
工作機會：jobs@bitdefender.com
病毒遞交：virus_submission@bitdefender.com
垃圾郵件遞交：spam_submission@bitdefender.com
報告濫用：abuse@bitdefender.com
產品網站：http://www.bitdefender.com
產品檔案FTP位址：ftp://ftp.bitdefender.com/pub
本地代理商：http://www.bitdefender.com/partner_list
BitDefender 知識庫：http://kb.bitdefender.com

27.3.2. 分公司

BitDefender辦公室已經準備好回應關於他們的任何諮詢，無論在商業或更大的事件。他們的地址和連絡方式在下面被列出。

美國

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
電話：1-954-776-6262
網站：http://www.bitdefender.com

技術支援。
■電子郵件：support@bitdefender.com
■免費電話：
- 美國：1-888-868-1873
- 加拿大：1-866-947-1873

消費者服務(限定已註冊的使用者)。
■電子郵件：customerservice@bitdefender.com
■免費電話：
- 美國：1-888-868-1873
- 加拿大：1-866-947-1873

德國

BitDefender GmbH

Airport Office Center
Robert - Bosch - Str. 2
59439 Holzwickede
德國
電話：+49 (0)231 99 33 98 0
電子郵件：info@bitdefender.com
業務相關：sales@bitdefender.com
網站：http://www.bitdefender.com
技術支援：support@bitdefender.com

英國及愛爾蘭

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
電話：+44 (0) 8451-305096
電子郵件：info@bitdefender.com
業務相關：sales@bitdefender.com
網站：http://www.bitdefender.co.uk
技術支援部門：support@bitdefender.com

西班牙

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
技術支援：soporte@bitdefender-es.com
業務相關：comercial@bitdefender-es.com
電話：+34 932189615
傳真：+34 932179128
網站：http://www.bitdefender-es.com

羅馬尼亞

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
技術支援部門：support@bitdefender.com
業務相關：sales@bitdefender.com

電話：+40 21 3001255
電話：+40 21 3001254
產品網站：http://www.bitdefender.com

BitDefender 救援光碟

28. 概觀檢視

BitDefender 網路安全2009 含有可開機光碟 (BitDefender 救援光碟是以LinuxDefender 為基準) 在您的作業系統啟動前，可進行掃描及清除所有存在的磁碟機。

您可以在您的作業系統因為病毒而無法運作時，使用 BitDefender 救援光碟。當您未使用任何病毒防護產品時，這種情形會常常發生。

病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

BitDefender 救援 CD提供一個桌面以供掃描及清除NTFS硬碟上的病毒之用。同時BitDefender在您不用進入可以Windows時，還原您的資料。



註
BitDefender救援光碟可於下列位置下載：http://download.bitdefender.com/rescue_cd/

28.1. 系統要求

在使用 BitDefender 救援 CD 開啟電腦前，您必須先確認您的系統符合以下的需求。

CPU 種類
: x86 相容機種、最少需要 166 MHz，但不能期望有很好的效能。i686 系列的處理器、800 MHz，可能運作的更有效率。

記憶體
: 最少 512MB 記憶體或以上 (建議使用1GB)

光碟機
: BitDefender救援光碟是由光碟機執行，因此，光碟機及可以從 BIOS 啟動開機為其要求項目。

網際網路連線
: 雖然BitDefender救援光碟是不需要在網際網路連線下執行，但更新的程序會要求啟動 HTTP 連線，甚至可以透過 Proxy 伺服器。因此，為了提供完整的防護，網際網路的連線是必需的。

圖形介面的解析度
: 標準 SVGA-相容圖像顯示卡

28.2. 包含的軟體

BitDefender 救援光碟包含以下的軟體程式。

Xedit
: 這是文字檔案編輯器。

Vim
: 這是更強的文字檔案編輯器，包含強調的語法格式，圖形用戶界面。要更多資訊，請參閱Vim網站。

Xcalc
: 這是計算機。

RoxFiler
: RoxFiler是一個快速而強大的圖形檔案管理員

  想要更多資料，請瀏覽 RoxFiler網站。

MidnightCommander
: GNU Midnight Commander (mc)是一個文字介面檔案管理員。

  想要更多資料，請瀏覽 MC網頁。

Pstree
: Pstree顯示正在執行的程序。

Top
: 上方顯示Linux工作區。

Xkill
: Xkill用來強制關閉系統中的任何一個應用程式。

Partition Image
: Partition Image幫您儲存整個分割區(EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32)至一個映像檔。此軟體能協助您備份。

  要更多資料，請瀏覽Partimage網頁.

GtkRecover
: GtkRecover是個GTK版本的檔案復原工具。它能助您挽回檔案。

  要更多資料，請參閱GtkRecover網頁。

ChkRootKit
: ChkRootKit能助您掃描電腦內的rootkit。



要更多資料，請參閱ChkRootKit 網頁.

Nessus Network Scanner

Nessus是一個Linux, Solaris, FreeBSD, and Mac OS X遠端安全掃描器。

要更多資料，請參閱Nessus網頁。

Iptraf

Iptraf是個IP網路監控軟體。

要更多資料，請參閱Iptraf網頁。

Iftop

Iftop顯示每個介面的頻寬用量。

要更多資料，請參閱Iftop 網頁。

MTR

MTR是一個網路診斷工具。

要更多資料，請參閱MTR網頁

PPPStatus

PPPStatus顯示TCP/IP流出流入的統計。

要更多資料，請參閱PPPStatus homepage。

Wavemon

Wavemon是一個無線網路裝置監控軟體。

要更多資料，請參閱Wavemon網頁。

USBView

USBView顯示已連接到USB bus的裝置資料。

要更多資料，請參閱USBView網頁。

Pppconfig

Pppconfig助您自動設置ppp撥號連線。

DSL/PPPoe

DSL/PPPoe 設置PPPoE (ADSL寬頻)連線。

I810rotate

I810rotate調節 i810硬件i810switch(1)的影像輸出。

要更多資料，請參閱I810rotate網頁。

Mutt
Mutt是一個強大的文字介面MIME郵件客戶端。

要更多資料，請參閱Mutt 網頁。

Mozilla Firefox
Mozilla Firefox 瀏覽器是一個大家耳熟能詳的網站瀏覽器。

要更多資料，請參閱Mozilla Firefox 網頁。

Elinks
Elinks是一個文字介面的網站瀏覽器。

要更多資料，請參閱Elinks網頁。

29. BitDefender 救援CD 說明

這一節會教您怎樣使用BitDefender 救援CD，掃描惡意程式無論電腦上已癱瘓不能開的Windows，以至隨插即用裝置。您更可以藉本CD做更多使用手冊上沒記載的事。

29.1. 啟動BitDefender 救援光碟

要啟動光碟，從BIOS設定您的電腦由光碟機啟動，放入光碟片並啟動電腦。確認您的電腦可以由光碟機啟動。

等待螢幕畫面出現，依循著畫面的指示去進行BitDefender 救援光碟。



註
從可用清單中選取您想要使用的語言。

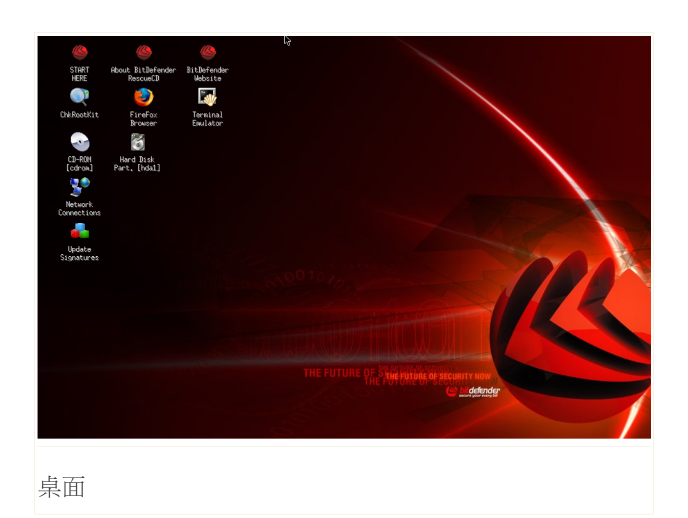


啟動畫面

病毒特徵碼的更新會自動進行，不需要在您每次啟動 BitDefender 救援光碟時再進行更新。

當啟動程序完成時，您將看到下一個桌面。您將開始使用BitDefender 救援CD 。

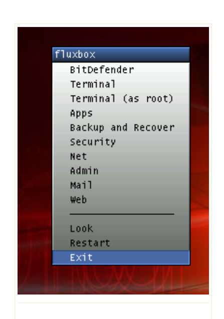




桌面

29.2. 停止BitDefender 救援光碟

在選擇離開 或執行halt指令後，您可以放心關機。



選擇 "離開"

當 BitDefender救援光碟已經成功關閉所有程式，它會顯示如以下的畫面。您可以從光碟機取出光碟片 。現在可以關閉您的電腦或重新開機。

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksusper
) (aio/0) Done.
Waiting for processes to finish.......................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd) (
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.......................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/ini
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes]._
```

等待這個訊息才關機。

29.3. 如何執行一個病毒防護掃描？

開機程序完成後，一個精靈便會出現。它會提示您掃描您的電腦。您只須點擊開始按扭。



註
若您的螢幕解析度不足，系統會問您是否要用文字模式掃描。

依照三步驟指引執行掃描任務。

1. 您能見到掃描狀態和統計（掃描速度，使用時間，掃描 / 受傳染的 / 可疑的 / 隱藏的物件和其他的數目）。

   註
   掃描程序將依它的複雜程度而需花費一些時間。

2. 您可以檢視可能影響您的系統的事件數量。

   結果會以群組顯示。 點擊 "+" 的小方框以展開選項或點擊 "-" 的小方框關閉選項。

   您可以針對不同的威脅類型的分組採取行動，也可以分別進行處理。

3. 您可以檢視結果。

如果您只想掃描某些特定資料夾，請依照下列步驟：

瀏覽您的資料夾，在檔案或目錄點擊滑鼠右鍵，選擇 傳送到。然後選擇 BitDefender 掃描器。

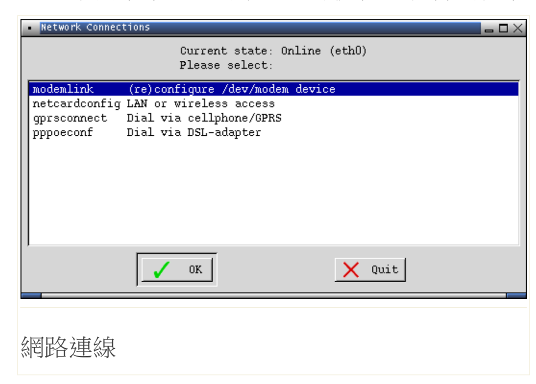
或者您可以用root執行下一個命令。BitDefender 病毒防護掃瞄開始掃描預設位置被選取的檔案或資料夾。

```
# bdscan /path/to/scan/
```

29.4. 如何設置網際網路連線？

如果您是在一個有 DHCP 的網路並且您有一塊網路卡，網際網路連線應該已經被偵測及設置。若要手動設定，請依照以下的步驟。

1. 點擊兩下桌面上的網路連線捷徑，將會出現下一個視窗。



網路連線

2. 選取您使用的連線類型並點擊確定。

連線	描述
數據機連線	當您使用數據機和電話線連線時，選取這個類型。
網路卡設置	當您使用區域網路時，選取這個類型。這同時也適用於無線網路。

連線	描述
GPRS連線	當您使用手機網路的GPRS (General Packet Radio Service)存取網路時，選取這個類型。
pppoe設置	如果您使用ADSL時，選取這個類型。

3. 請依照畫面的指示。如果您不確定答案，請與您的系統或網路管理者詢問。



重要

請注意您只有在選取了上述的選項之後才能啟動數據機。要設置網路連線請依照下列步驟。

1. 在桌面點擊右鍵，BitDefender救援CD 右鍵選單將會彈出。
2. 選取終端機(作為root)
3. 輸入下列指令：

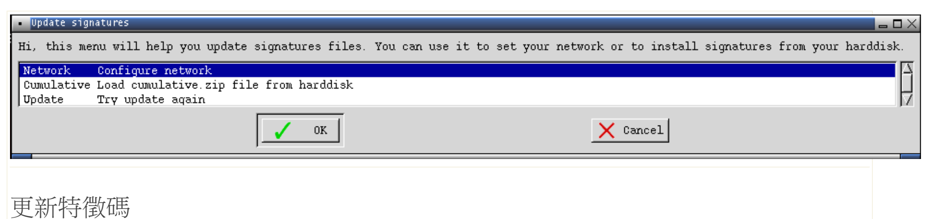
```
# pppconfig
```

4. 請依照畫面的指示。如果您不確定答案，請與您的系統或網路管理者詢問。

29.5. 如何更新BitDefender？

啟動電腦時會自動進行病毒特徵碼的更新。

1. 在桌面上的更新特徵碼捷徑點擊右鍵，將會出現下一個視窗。



更新特徵碼

2. 您可以選擇以下動作：
   - 選取累積以安裝以儲存在您的磁碟上以及透過載入cumulative.zip取得的特徵碼。。
   - 選取更新以立即連線至網際網路並取得最新的病毒特徵碼。

3. 點擊確定。

29.5.1. 如何使用proxy伺服器更新BitDefender？

若您的電腦要使用proxy伺服器才能上網，您須要做一些設定，才能更新病毒特徵碼。

要經proxy伺服器更新，請依照下列步驟。

1. 在桌面點擊右鍵，BitDefender救援CD 右鍵選單將會彈出。
2. 選取終端機(作為root)
3. 輸入以下命令：cd /ramdisk/BitDefender-scanner/etc。
4. 輸入以下命令：mcedit bdscan.conf以GNU Midnight Commander (mc)編輯這個檔案。
5. 解除這行的註解#HttpProxy =(只是刪去#號)，再打網域，使用者名稱，密碼，伺服器連接埠。例如，這幾行一定像這樣：

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. 按下F2以儲存目前的檔案，然後點擊 F10關閉它。
7. 輸入這個命令bdscan update。

29.6. 如何儲存我的資料？

假設您因一些不知名的原因導致您不能進入Windows。同一時間，您一定得要存取一些重要的資料。這就是使用BitDefender救援CD 的時候了。

要從您的電腦取得資料並移動到卸除式磁碟，例如USB隨身碟，請依照下列步驟：

1. 將BitDefender救援CD放入光碟機，將隨身碟插入USB槽，然後重新開機。



註

如果您稍後拔出了隨身碟，您必須以照下列步驟掛載它：

a. 在桌面上的終端機模擬器捷徑點擊兩下。

b. 輸入下列命令：

```
# mount /media/sdb1
```

請注意，隨著您的電腦設置不同，它可能是sda1而不是sdb1。

2. 等到 BitDefender救援CD 完成開機。將會出現下一個視窗。



桌面

3. 點擊兩下您想復原的資料所屬的硬碟分割區(例如：[sda3]).



註

在 BitDefender救援CD 中，硬碟分割區會使用Linux-type名稱。所以[sda1]可能對應Windows-type中的(C:)，而[sda3] 對 (F:)，以及 [sdb1]指向隨身碟。



重要

如果電腦沒有正確的關機，有可能某些磁碟分割沒有自動載入。要載入磁碟分割，請依照下列步驟。

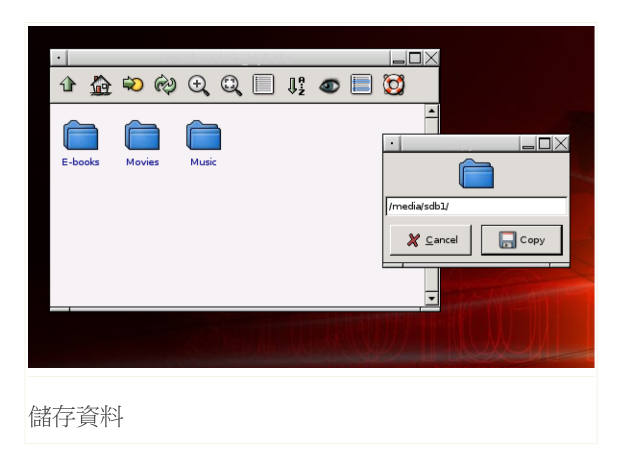
a. 在桌面上的終端機模擬器捷徑點擊兩下。

b. 輸入下列命令：

```
# mount  /media/partition_name
```

4. 瀏覽您的資料夾。例如：我的資料 包含 影片， 音樂 和 E-books子資料夾。

5. 在您想要的目錄上點擊右鍵，選取複製，將會出現下一個視窗。



儲存資料

6. 輸入/media/sdb1/至對應的欄位，然後點擊複製。

請注意，隨著您的電腦設置不同，它可能是sda1而不是sdb1。

詞彙表

ActiveX

ActiveX是一個程式模型讓其他程式和作業系統執行它們。ActiveX技術是用來給微軟Internet Explorer令動態網頁比靜態網頁看起來更像電腦程式。藉由 ActiveX ，使用者能使用按鈕，和其他網頁中的互動元件詢問問題或回答問題，。 ActiveX 控制時常使用 Visual Basic 編寫。

ActiveX 對完全缺乏安全管控的電腦是值得注意的；電腦安全專家對它在網際網路上的ActiveX也感到沮喪。

廣告軟體

廣告軟體通常包含在一些應用程式。這個軟體不會經使用者同意才安裝。因為這些廣告軟體在同意版權合約之後就安裝，這也是這個軟體的目的，而這個過程沒有犯罪。

然而，自動彈出的廣告能變成一種煩惱，同時也會降低電腦的效率。同時，這些軟體所收集的資料可能會涉及個人隱私而安裝授權沒有完全記載。

資料封存

一個磁片 、磁帶或目錄，包含了已經備份的檔案。

檔案裡包含一個或多個以壓縮格式存在的檔案。

後門

一個系統設計者或管理員故意留下的安全漏洞，不是每個漏洞都是不好的。例如：伺服器支術員或代理商的維護電腦程式編寫員都希望要有個有特權的帳號。

開機磁區

每個硬碟的開頭都儲存了這隻硬碟的結構，(磁區大小、叢集大小等等)。若是開機硬碟，開機磁區包含着一個程序使開機時載入作業系統。

開機型病毒

一種在硬碟或磁碟上使開機磁區受感染的病毒。由磁碟開機然後蔓延至記憶體上。每次您開機，您就會啟動在記憶體的病毒。

瀏覽器

網站瀏覽器的簡稱，這個軟體用來顯示網頁。目前二大最受歡迎的瀏覽器是 Netscape Navigator 及 Microsoft Internet Explorer。二者都是圖形化介面的瀏覽器，代表它們同時可以顯示圖片及文字。除此之外，在加入其他的程式元件，也可以顯示多媒體資訊，包含聲音、影片。



命令列
: 在命令列介面，使用者可以直接在畫面輸入命令

Cookie
: 在網際網路中，cookies是有關個別電腦資訊的小檔案，它又能被分析而且能被廣告界使用者追蹤您的關於上網的興趣和品味。在這範圍，cookies技術仍然繼續發展，而且意圖直接地把您感興趣的廣告瞄準著您。這是一把雙面刃。因為一方面，這種技術會更有效率，因為您只會看到您感興趣的廣告。另一方面，事實上，它會「追蹤」並「跟隨」您去了哪和按了什麼鍵。可理解地，這有隱私上的爭論，他們覺得被網站看作"SKU數字" (就好像在包裝紙上的條碼)的辯論。當然這樣的觀點是極端的，但是在某些情況下是正確的。

磁碟機
: 磁碟機可允許讀取資料及寫入資料。

硬碟機可以讀取及寫入資料到硬碟。

軟碟機可以存取磁碟片。

硬碟機有包含內接式 (放置在電腦主機內) 或外接式 (放置在一個獨立的機殼裡，並與電腦主機連線)。

下載
: 要把資料(通常全部檔案)從一個主要的來源複製到週邊裝置。這詞語通常用來形容從線上服務到某人的電腦上。下載通常看成從網路上的檔案伺服器複製到一部電腦上。

電子郵件
: 電子郵件。經由本地或全球網路在電腦上傳遞郵件的服務。

事件
: 由軟體偵察到的一個動作或事件。事件可以是使用者的動作，例如：用滑鼠點擊或按鍵盤上的按鍵或系統事件，例如：記憶體用完。

誤判
: 當掃描器識別出一個檔案受到感染，而事實上並不是。

副檔名
: 檔案名稱的一部份，它會跟隨在一個 "." 之後，它指出檔案是何種類型的資料。

許多作業系統使用副檔名，如：Unix、VMS 及 MS-DOS。它們通常含有一到三個字元。例如：c 代表 C 語言的原始檔、ps 則是 PostScripts 格式、txt 則是文字檔。

啟發式技術

識別新的病毒的基礎方法。這類的掃描不依賴特定的病毒特徵碼。好處是不會被舊病毒的變種愚弄。然而，它可能有時在正常的軟體中報告有該軟體懷疑是病毒。產生所謂的「誤判」。

IP

網際通訊協定－在TCP/IP中的一組通訊協定可定路線通訊協定。負責IP位址，決定路徑和IP 封包的分拆和合併。

Java applet

一個Java程序，它設計用來只是在網頁上執行。要在網頁上使用applet，您需要先定好applet的名，大小(長和寬，以像素為單位)來讓applet應用。當存取網頁時，瀏覽器會從伺服器下載applet，並在使用者的電腦上執行。Applet和其他的軟體分別在於Applet有嚴格的通訊協定。

例如：即使Applet在客戶端上執行，它也不能讀寫客戶端上的資料。此外，Applet在網路上有著更嚴格的監管。他們只能讀寫同一網域上的資料。

巨集型病毒

這類型的病毒是在檔案中含有巨集程式。許多應用程式如：Microsoft Word 及Excel，都有支援巨集語言。

這些應用程式允許您在一個檔案裡插入一個巨集，在檔案每一次被開啟時，巨集程式即可被執行。

電子郵件程式

一個電子郵件程式是一個應用程式，它讓您可以傳送及收發電子郵件。

記憶體

電腦內部的儲存空間，這詞語指資料被儲存為很多小碎片。而「儲存」這個詞語是指已經在磁帶或者硬碟內。每部電腦都有一定數量的實體記憶體。通常我們通稱它為主記憶體或RAM。

非啟發式技術

這個方法是依賴特定的病毒特徵碼。非啟發式技術的好處是它不會把相似的當是病毒，以及它不會彈出錯誤的警告。

壓縮程式

一個被壓縮的檔案格式。很多作業系統和應用程式包含這個命令使您把格案壓縮減少使用的記憶體。例如：您有一個文字檔案包含著十個連續的空格。通常，會用十個位元組(bytes)來儲存。

然而，程式會把檔案壓縮，用一特定空格組合字元取代空白字完。在這個情況，十個空格字元會被取代成二個位元。這只是其中一隻壓縮技術，還有其他很多種。

路徑

在電腦裡一個檔案確切的位置。 根據等級制度檔案系統，這些方向通常描述從上到下。

兩點之間的路徑，例如：兩電腦之間的通訊頻道。

網路釣魚

將一份電子郵件送到一個使用者，並虛偽地自稱是合法的企業，並要求受害者主動地提交自己的個人資料，使犯人竊盜受害者的私人的資料。電子郵件指示使用者到一個像合法的組織的網站，更新個人的資料， 像是密碼和信用卡、社會福利和銀行帳號的網站。然而，網站是假的，只是建立起來用來偷使用者的資料。

多形病毒

病毒會改變它的形式來傳染每個檔案。因為他們沒有一致的二進制樣式，這樣的病毒很難辨認。

連接埠

一個連接埠在您能連接設備的電腦。　 個人電腦有的連接埠各種各樣的類型。內部，有幾個連接埠用來連接的磁碟機、螢幕和鍵盤。外接，個人電腦有連接埠用來連接的數據機、印表機、滑鼠和其他外接設備。

在TCP/IP和UDP網路，一個終點對邏輯連接。連接埠號碼用來辨認它是哪一個連接埠。 例如，連接埠80為HTTP傳輸使用。

報告檔案

這個檔案列出 BitDefender 發生的行為。BitDefender 在報告檔裡列出掃描的路徑、目錄、掃描的檔案數量及被掃描的檔案，有多少受感染及可疑檔案被發現。

Rootkit(後門程式)

rootkit是一套提供系統的管理員層級存取的軟體工具。首次出現在UNIX作業系統，並且提供了入侵者管理權利的重新編譯的工具，使他們隱藏不被系統管理員看見。

rootkits的主要角色是掩藏程序、檔案、註冊和日誌。　 如果他們合併適當的軟體，他們也許也能攔截資料從終端、網路連接或者外圍設備。

Rootkits本質不是惡意的。例如，系統和有些應用使用rootkits掩藏重要檔案。然而，他們主要用於掩藏惡意程式或隱瞞入侵者已經入侵系統。 當與惡意程式結合時，　 rootkits造成巨大威脅和系統的安全。他們可以監測工具，建立後門系統，修改檔案和日誌和避免偵查

Script

有別於巨集或批次檔案，script 是一連串要被執行的命令，而且不需要使用者介入。

垃圾郵件

電子郵件廣告或垃圾新聞群組。通常被認為是任何未經同意的電子郵件。

間諜程式

透過使用者的網際網路連結收集資料，而通常作為廣告用途。間諜程式通常都隱藏在免費軟體的一個元件中，所以很容易被使用者下載；然而大部分的免費軟體其實是沒有間諜程式的。一旦安裝之後，間諜程式監控您的在網際網路上的動作並秘密地將資訊傳送到某處。間諜程式同時也收集有關電子郵件地址甚至是密碼、信用卡號碼等資訊。

間諜程式和木馬程式的相似之處是使用者都在安裝其他軟體時無意安裝了它們。在點對點的傳輸軟體中相當常見。

除了道德和隱私問題之外，間諜程式也占據了電腦的記憶體以及網際網路頻寬。由於間諜程式使用了您的系統資源，可能會造成您的電腦當機或系統不穩定的問題。

啟動項目

當電腦啟動，在這個資料夾的所有檔案將會開啟。例如，一個啟動畫面、第一次啟動電腦的音效檔案、一個提醒日曆或一個應用程式。 通常，檔案的別名在這個資料夾而不是檔案位置。

系統工具列

介紹與Windows 95，系統鍵盤位於視窗工作列(通常在底部的時鐘旁邊)並且包含小型圖示以簡易地存取某些系統工作，例如傳真、印表機、數據機、音量控制。點擊兩下或點擊右鍵圖式以檢視和存取細節和管控。

TCP/IP

傳輸控制通訊協定－一套網路通訊協定用途廣泛在提供通訊橫跨電腦在互聯的網路以不同的硬體結構和各種各樣的作業系統的網際網路。 TCP/IP包含電腦溝通標準和連接網路的協定。

木馬程式

一種偽裝成良性程式的破壞性程式。不同於病毒，木馬程式不複製自己，但是他們具破壞性。其中一個電腦程式內的病毒的最陰險的類型是趕走您的電腦病毒，但是又引進其他病毒。

這個詞的來源來自荷馬史詩，希臘人送了一匹巨型木馬給他們的仇敵，特洛伊人，表面上作為和平獻禮。 但在特洛伊人將木馬拉入在他們的城市之後，希臘戰士偷偷地從木馬中爬出來並打開城門，讓他們的同胞湧入並抓住特洛伊。

更新

一個軟體或硬體產品的新版本，設定用來取代相同產品的舊版本。此外，更新的安裝規則需要先去檢查是否已經存在一個舊版本在您的電腦，如果不是，您無法安裝這個更新。

BitDefender 擁有它自已的更新模組，它允許您手動檢查更新，或者讓它自動地更新軟體。

病毒

您的電腦没有您的了解和運作時被裝載某程式或一些代碼。多數病毒能複製自己。所有電腦病毒都是人造的。簡單的病毒能複製自己和相對地容易製造。 因為它將迅速使用所有可利用的記憶體並且影響效能，這樣簡單的病毒對系統是危險的。一個更加危險類型的病毒是一個橫跨網路能傳送並繞過安全系統。

病毒定義

病毒的二進位典型，被防毒軟體用來偵測並刪除病毒。

蠕蟲

一個在網路之上繁殖它本身的程式。它不能夠把它本身附在其他的程式。